НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра автоматики та управління в технічних системах

«До захисту допущено»

Завідувач кафедри

_____ О.І. Ролік

«___»_____2019 р.

Дипломний проект

на здобуття ступеня бакалавра

з напряму підготовки 6. 050201 «Системна інженерія»

на тему: «Система управління об'єктом з критичними інформаційними ресурсами»

Виконав:
студент IV курсу, групи ІА-51
Заболотний Владислав Валерійович _____

Керівник:
Професор кафедри АУТС, доктор технічних наук,
доцент, Корнієнко Б.Я. _____

Рецензент:
Доцент кафедри АУТС, кандидат технічних наук,
доцент, Павлов В.Г. _____

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2019 рік

Пояснювальна записка
до дипломного проекту
на тему: «Система управління об’єктом з критичними інформаційними ресурсами»

Київ – 2019 рік

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 4
ВСТУП 5
1 АНАЛІЗ ПОБУДОВИ ТА ЗАГРОЗ СУЧАСНИХ АСУ ТП 8
1.1 Сучасні АСУ ТП 9
1.2 Типова структура АСУ ТП 11
1.3 Склад АСУ ТП 12
1.3.1 SCADA-система 13
1.4 Телекомунікації у промислових АСУ ТП 14
1.4.1 Мережі нижнього рівня АСУ ТП 14
1.4.2 Промислові мережі верхнього рівня АСУ ТП 15
1.5 Загрози інформаційній безпеці в АСУ ТП 15
1.5.1 Класифікація інформаційних загроз АСУ ТП 16
1.6 Уразливості промислових систем 20
Висновки до розділу 1 22
2 БЕЗПЕКА В АСУ ТП 23
2.1 Загальні відомості 23
2.2 Математична модель впливу загроз на ІС 28
2.2.1 Приклад числової реалізації моделі 31
2.2.2 Приклад числової реалізації моделі 33
Висновки до розділу 2 34
3 УПРАВЛІННЯ АСУ ТП З ВРАХУВАННЯМ БЕЗПЕКИ 35
3.1 Вибір засобів безпеки 42
3.2 Заходи безпеки для АСУ ТП 43
3.3 Захист локальної мережі АСУ ТП 46

3.4 Вимоги до персоналу АСУ ТП 48
3.5 Оцінка ризику та плани у випадку надзвичайних ситуацій 49
3.6 Контроль доступу до АСУ ТП 53
Висновки до розділу 3 59
ВИСНОВКИ 60
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 61
ДОДАТОК А 63

ПЕРЕЛІК СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце

АС – автоматизовані системи

АСУ – автоматизована система управління

АСУ ТП – автоматизована система управління технологічним процесом

ІБ – інформаційна безпека

ІС – інформаційна система

КЗЗ – комплекс засобів захисту

ЛЗ – лінія зв’язку

НСД – несанкціонований доступ

ЗМЗ – зовнішні мережі зв’язку

ОС – операційна система

ПК – персональний комп’ютер

ПЛК – програмований логічний контролер

ПЗ – програмне забезпечення

СЗІ – система захисту інформації

СЗІ НСД – система захисту інформації від несанкціонованого доступу

ЛОМ – локальна обчислювальна мережа

РСК – розподілені системи контролю

ВСТУП

У сучасному світі автоматизовані системи управління (АСУ) використовуються все частіше і частіше. Необхідність забезпечення інформаційної безпеки у автоматизованих системах управління зростає з кожним роком через збільшення кількості атак зловмисників та витоки конфіденційної інформації. Але найбільш чутливими до безпеки є саме автоматизовані системи управління технологічними процесами (АСУ ТП) так, як при атаці зловмисників, може статися не тільки витік секретної інформації, а й втручання в сам технологічний процес, який, при збої, може призвести до екологічної катастрофи.

Управління технологічними процесами у підприємствах малого, середнього та великого розміру неможливе без обчислювальної техніки та сучасних засобів автоматизації, без високоефективних автоматизованих систем управління технологічними процесами (АСУ ТП).

АСУ – це комплексна система апаратного та програмного забезпечення, яка призначена для віддаленого централізованого слідкування за станом процесів та системи в цілому, а також для автоматизованого керування інженерними та технічними підсистемами підприємств з диспетчерського пункту, підтримки рішень під час експлуатації системи[1].

Актуальність цього бакалаврського проекту пов’язана з широким використанням телекомунікацій в АСУ ТП і високим рівнем небезпеки загроз підміни, викривлення, втрати інформації та інших. При проектування та експлуатації АСУ ТП, обов’язково повинен виконуватись постійний аналіз системи на справність, надійність та стійкість до небезпек.

Забезпечення інформаційної безпеки (ІБ) АСУ ТП стає все актуальнішим питанням з розвитком обчислювальної техніки та все більшим проникненням таких систем у повсякденне життя людей. Це обговорюється майже на кожному заході з забезпечення ІБ, а проведення аналізу надійності та безпеки систем, які вже введені в експлуатацію, є однією з обов’язкових умов державної та міжнародної сертифікації. Однією з найбільших проблем забезпечення ІБ є те, що

більшість АСУ малої та середньої складності проектуються малими організаціями в умовах жорсткої фінансової обмеженості, що нівелює або сильно ускладнює питання забезпечення ІБ[2].

Експерти впевнені, що забезпечення ІБ АСУ відрізняється від забезпечення ІБ корпоративних інформаційних систем. Навіть сам термін “інформаційна безпека” дуже рідко використовується у відношенні АСУ ТП. Причиною цьому є те, що необхідно приділяти увагу не стільки конфіденційності інформації, а забезпеченню неперервності та цілісності самого технологічного процесу. Хоча у той самий час значна кількість уваги приділяється проблематиці забезпечення конфіденційності інформації, бо, на думку багатьох експертів, вирішення цієї проблеми веде до автоматичного вирішення проблеми цілісності та доступності інформації.

Сучасні АСУ у багатьох випадках керують складними та небезпечними технологічними процесами, збій у яких потенційно може призвести до аварій на виробництві або, у найгіршому випадку, до техногенних катастроф. Це значно збільшує ціну ризиків через порушення ІБ, бо реалізація загроз теоретично може призвести до вчинення шкоди людям, навколишньому середовищу, а також беззаперечно веде за собою фінансові та репутаційні втрати.

У сучасні часи, пріоритетом у забезпеченні ІБ АСУ ТП є забезпечення доступності та цілісності управляючої та конфігураційної інформації про параметри технологічного процесу. Особливу увагу потрібно звертати на запобігання несанкціонованого доступу до системи для збереження стійкого функціонування АСУ ТП.

Цей дипломний проект досліджує інформаційну безпеку АСУ ТП: будуть досліджені мережні нижчого рівня на предмет загрози конфіденційності та цілісності інформації, яка передається мережею; буде проведений аналіз мереж зв’язку АСУ ТП на можливі загрози та уразливості; створена математична модель загроз; будуть розроблені додаткові заходи для захисту цілісності та конфіденційності даних.

У цьому проекті усі наукові дослідження засновані на методах математичного моделювання, математичної статистики, експертних оцінок з широким використанням програмно-математичних засобів. Основні теоретичні результати перевірені в конкретних системах та з допомогою моделюючих програм з допомогою сучасних обчислювальних засобів.

1 АНАЛІЗ ПОБУДОВИ ТА ЗАГРОЗ СУЧАСНИХ АСУ ТП

У цьому розділі розглядаються сучасні методи побудови АСУ ТП. Враховуючи результат аналізу побудови автоматизованих систем, проектовані на об’єктах АСУ ТП будуть позбавлені можливих загроз інформаційної безпеки, яким схильні сучасні промислові системи.

Актуальність цієї роботи пов’язана з широким використанням телекомунікацій в АСУ ТП і високим рівнем небезпеки викривлення чи втрати інформації. Готовність організацій і підприємств, що розробляють та експлуатують АСУ ТП, виконувати аналіз їх надійності і безпеки є однією з ключових вимог державної та міжнародної сертифікації. Однак більшість систем управління технологічними процесами проектуються малими організаціями з скрутних фінансових та кадрових умовах. Часто в таких умовах питаннями інформаційної безпеки не займаються зовсім[13].

Якщо в атомній промисловості та енергетиці наслідки порушення безпеки, у тому числі й інформаційної, можуть бути масштабними і катастрофічними, то масштаб шкоди в АСУ ТП хімічної промисловості далеко не завжди такий великий та очевидний. Розмір шкоди та її характер визначається саме самим технологічним процесом. При системному підході потрібно розглядати систему управління у взаємозв’язку та взаємовпливі не тільки з об’єктом управління (у цьому випадку – технологічним процесом), а з джерелами енергії, навколишнім середовищем. У хімічній промисловості вплив на навколишнє середовище обов’язково повинен піддаватись серйозному аналізу не тільки в аварійному, але й у звичайному, нормальному режимах роботи АСУ ТП. Згубний вплив на екологію може бути викликаний не тільки витоками і технологічними викидами шкідливих речовин, а й, наприклад, зміною температури води у водоймі при охолодженні або викиді у неї технологічної води, забраної з артезіанської свердловини.

Забезпечити ІБ АСУ ТП на достатньо високому рівні, при постійно зростаючому рівні інформатизації і збільшення кількості загроз, уже неможливо

лише з комплексом зовнішніх механізмів захисту. Пропонується такий підхід до ІБ АСУ ТП, коли внутрішню захисну оболонку буде створювати комплексна система ІБ, а внутрішні бар'єри створюють вбудовані механізми захисту програмних та технічних компонентів АСУ ТП. Такий підхід можна назвати системним.

Обійти зовнішній захист можна, внутрішній – набагато важче. Саме тому звертається особлива увага на переваги розробки і використання програмних і апаратних засобів АСУ ТП, які мають вбудовані механізми захисту, який оператор може управляти для створення потрібної пропорції механізмів захисту у системі захисту інформації[3].

Засоби телекомунікацій в АСУ ТП – це різноманіття апаратури і програмного забезпечення, які повинні мати внутрішні механізми власної безпеки. Саме тому від виробників технічних засобів і програмного забезпечення АСУ ТП потрібна розробка інструментів забезпечення безпеки своїх продуктів.

1.1 Сучасні АСУ ТП

Для будь-якого підприємства чи організації збільшення ефективності виробництва у першу чергу визначається ефективністю існуючої системи управління. Завдання скоординованої взаємодії всіх підрозділів, оперативної обробки і аналізу отриманих даних дозволяє вирішити впровадження сучасної АСУ[1].

Дуже важливо робити акцент саме на терміні "автоматизована". Це поняття означає те, що у система управління потребує оператора для реалізації завдань, а це означає, що вона не є повністю автономною. Якщо ж потрібна система управління, що працює автономно без втручання та будь-якого контролю зі сторони людини, то використовують системи автоматичного управління (САУ).

АСУ ТП відноситься до класу складних систем, яким властиві наступні ознаки:

– наявність у всіх елементів загальної цілі

– системний характер алгоритмів обміну та обробки інформації, які реалізуються
– велика кількість складових функціональних підсистем

Досліджуючи проблеми ІБ, ми будемо розглядати АСУ на різних рівнях взаємодії її компонентів.

Забезпечення конфіденційності та захист інформації на вході, виході, передачі, обробці та зберіганні, а також протидія її викраденню, знищенню чи спотворенню є однією з найважливіших особливостей АСУ. Об'єктом захисту є дані, які містять конфіденційну інформацію та будь-які дані, які зберігаються, обробляються та передаються між різними елементами АСУ ТП. Через ріст інтересу зловмисників до подібних систем управління, який постійно збільшується, все більш актуальним стає питання захисту інформації, які обробляється АСУ[5].

Експерти з безпеки вважають, що без забезпечення конфіденційності інформації, такого терміну як "безпека" взагалі бути не може. З одного боку, конфіденційність даних ніяк безпосередньо не впливає на роботу самої АСУ ТП. Важко уявити як розголошення інформації про технологічний процес може негативно вплинути на сам процес або вивести його з ладу. З іншого боку, незахищені та некоректні дані можуть вплинути на розвиток небажаних соціальних наслідків як от розголошення інформації про датчик радіації на АЕС, який вийшов з ладу.

У момент своєї появи, АСУ були лише ізольованими автоматизованими системами, які функціонували на базі вузькоспеціалізованого програмного забезпечення та обладнання. Тому у ті часи проблема забезпечення інформаційної безпеки повністю забезпечувалась роботою з персоналом та фізичних захистом компонентів самої системи.

З плином часу, автоматизовані системи розвинулись до такого рівня, що все частіше з'являлась потреба інтеграції з корпоративною інформаційною інфраструктурою для забезпечення взаємодії з різними бізнес-додатками і підтримки віддаленого доступу до системи. Іншими словами, автоматизовані

системи отримали доступ до глобальної мережі, це дозволило збільшити сферу їх використання, зробити зручнішою їх інтеграцію у загальні бізнес-структури, але також і зробило їх вразливими до нових ризиків, які були невідомі для них раніше, але були давно відомі традиційним IT-системам[4].

1.2 Типова структура АСУ ТП

Ряд компаній зараз пропонують комплексні рішення в області засобів автоматизованого управління технологічними процесами, але незалежно від розробника, всі сучасні АСУ ТП будуються на єдиних загальноприйнятих принципах.

В АСУ ТП можна виділити три рівні.

Нижній рівень – це рівень апаратних давачів – давачі, пристрої вимірювання технологічних параметрів, приводи та виконавчі пристрої, встановлені на технологічному обладнанні і призначені для збору первинної інформації і реалізації виконавчих впливів. Цей рівень також має назву “польовий” або рівень “вводу/виводу”(I/O). Якщо деякі або всі пристрої нижнього рівня є інтелектуальними, обмін інформації між ними може здійснюватися безпосередньо за допомогою мережі передачі даних[2].

Середній рівень – це рівень програмованих логічних контролерів (ПЛК) і пристроїв з’єднання об’єктів. Їх головною функцією є безпосереднє автоматизоване управління технологічними процесами. Управління виконавчими механізмами здійснюється за допомогою спеціальних алгоритмів шляхом обробки даних про стан технологічних параметрів, отриманих від вимірювальних пристроїв. Цей рівень також називають “рівень безпосереднього управління”.

Верхній рівень реалізується за допомогою персональних комп’ютерів (ПК), які виконують роль автоматизованих робочих місць (АРМ), де з допомогою спеціальних програмних пакетів (SCADA систем) реалізується інтерфейс з оператором-технологом, які виконує моніторинг і безпесереднє керування технологічним процесом.

На рисунку 1. Представлена типова структурна схема трьохрівневої АСУ ТП.

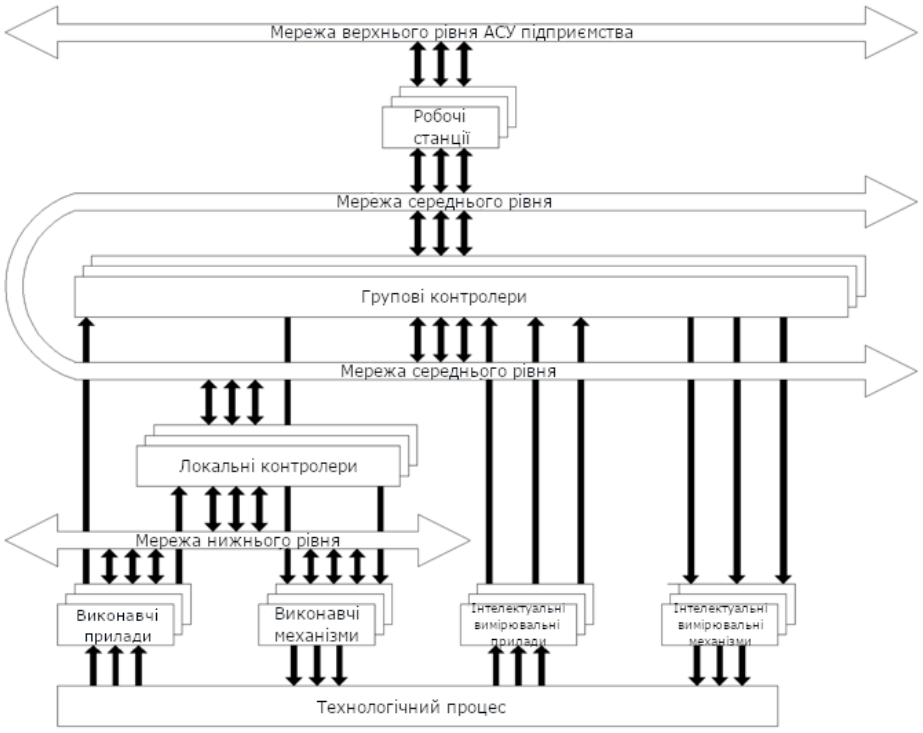

Рисунок 1.1 – Типова структурна схема трьохрівневої АСУ ТП

1.3 Склад АСУ ТП

Для функціонування АСУ ТП потрібна взаємодія наступних компонентів:

- технічне забезпечення
- програмне забезпечення (ПЗ)
- інформаційне забезпечення
- організаційне забезпечення
- операційний персонал

Технічним забезпеченням АСУ ТП називають повну сукупність технічних засобів, достатніх для функціонування АСУ ТП і реалізації системою всіх її функцій.

Програмне забезпечення АСУ ТП – це сукупність програм, які необхідні для реалізації функцій АСУ ТП, заданого функціонування комплексу технічних

засобів АСУ ТП та прогнозованого розвитку системи.

Інформаційне забезпечення АСУ ТП складається з:

– інформації про стан технологічного процесу
– системи класифікації і кодування технологічної і техніко-економічної інформації
– масивів даних і документів

Організаційне забезпечення АСУ ТП – це сукупність описів функціональної, технічної і організаційної структур та інструкцій для операційного персоналу АСУ ТП, яка забезпечує задане функціонування операційного персоналу.

До операційного персоналу відносяться технологи-оператори і експлуатаційний персонал, які забезпечують правильне функціонування комплексу технічних засобів.

Одним з головних технічних компонентів АСУ ТП є SCADA-система і програмовані логічні контролери.

1.3.1 SCADA-система

SCADA-система (від англ. Supervisory control and data acquisition, укр. – диспетчерське управління та збір даних) – це програмний пакет, призначений для розробки чи забезпечення роботи у режимі реального часу систем збору, обробки, відображення та архівування інформації про об’єкт моніторингу чи управління.

Зараз існує багато варіантів SCADA-систем різного роду та призначення. Проектуючи АСУ ТП для конкретного об’єкту та обираючи SCADA-систему, потрібно також опиратись на рівень захисту поміж інших критеріїв вибору.

Основними та найбільш популярними SCADA-система сьогодні є SIMATIC WINCC компанії Siemens (Німеччина) та INTOUCH компанії Wonderware (США). На ринку також існує безліч інших SCADA-систем, які майже по своїх функціональних можливостях та засобах підтримки безпеки нічим не відрізняються від двох згаданих раніше.

У Додатку А наведене порівняння згаданих вище найпопулярніших SCADA-систем та системи від незалежних розробників OpenSCADA.

1.4 Телекомунікації у промислових АСУ ТП

Мережі передачі даних, які входять у склад АСУ ТП, можна умовно розділити на два класи: мережі нижнього рівня (польові шини) та мережі верхнього рівня.

1.4.1 Мережі нижнього рівня АСУ ТП

Промислові мережі передачі даних – базовий елемент для побудови АСУ ТП. Саме поява промислових комунікаційних протоколів стало одним з чинників початку використання територіально розподілених систем управління, які здатні охопити безліч технологічних установок і процесів.

Головною функцією польової шини є забезпечення мережевої взаємодії між контролерами і віддаленої периферією. Також до польової шини можуть підключатись інтелектуальні пристрої, якщо вони підтримують високорівневі протоколи мережевого обміну.

Найчастіше використовують такі протоколи мереж зв’язку для нижнього рівня:

– Modbus RTU
– Modbus ASCII
– Profibus DP
– Profibus PA

Незважаючи на наявність особливостей кожного з стандартів (швидкість передачі, формат кадру, фізичне середовище), у всіх них є спільна особливість – алгоритм мережевого обміну даними, заснований на класичному принципі Master-Slave (головний-підпорядкований) (Profibus PA – лише один підпорядкований). Як лінія зв’язку використовується екранована вита пара, довжина кадру – 246

байт, а максимальна кількість контрольованих вузлів не перебільшує 127 (для Profibus PA - 32). Практично всі існуючі протоколи мають апаратну реалізацію перших двох рівнів моделі OSI (фізичний і канальний рівні). У мережах АСУ ТП нижнього рівня у всіх стандартах зв'язку реалізований захист даних CRC-кодом.

1.4.2 Промислові мережі верхнього рівня АСУ ТП

Мережі верхнього рівня використовуються для передачі даних між контролерами, серверами та робочими станціями. Основний стандарт мереж верхнього рівня – Ethernet (IEEE 802.3). Причина широкого використання цього стандарту зрозуміла: за допомогою Ethernet легко об'єднують обладнання верхнього рівня АРМ і сервери, які у більшості випадків є персональними комп'ютерами. Також перевагою мереж Ethernet є велика швидкість передавання даних.

У програмного комплексі АСУ ТП і мережах верхнього рівня використовуються такі заходи з захисту: ведення архіву повідомлень, захист інформації вбудованими інструментами протоколу Ethernet, самодіагностика програмно-технічних засобів, захист від несанкціонованого доступу за допомогою паролю.

1.5 Загрози інформаційній безпеці в АСУ ТП

У цьому розділі розглянуті найбільш поширені загрози, які властиві сучасним АСУ ТП[5], а в якості прикладу (у наступному розділі) буде показана справжня проектована АСУ ТП. Промислові АСУ ТП, на відміну від інших автоматизованих інформаційних систем, особливо від тих, які використовуються для управління критичною інфраструктурою та процесами на рівні держави, мають ряд особливостей, зумовлених їх особливим призначенням, умовами експлуатації, специфікою інформації, що обробляється, та вимогами, які вимагаються від їх функціонування. Головною особливістю таким систем є те, що

з їх допомогою в автоматичному або автоматизованому режимі в реальному часу здійснюється управління фізичними процесами і системами, від яких може залежати наша безпека і життєдіяльність. Це може бути будь-яке виробництво як атомне чи хімічне або системи життєзабезпечення, електростанції.

Сучасні промислові АСУ будуються на вже стандартному обладнанні (стандартні IT-платформи, SCADA-системи) і, у більшості випадків, для підвищення ефективності управління, підключаються до суміжних систем. Завдяки такій стандартизації, а також відкритості систем, збільшується вразливість АСУ до кібератак[11].

1.5.1 Класифікація інформаційних загроз АСУ ТП

Для вибору (чи розробки) оптимального засобу забезпечення безпеки потрібно мати уявлення про всі можливі загрози (як зовнішні, так і внутрішні) та про місця, які особливо їм підвладні.

Загрози, як і все у інформаційній безпеці, залежать від інтересів суб'єктів інформаційних відносин і від того, яка шкода для них вважається прийнятною.

Класифікація загроз за різними критеріями[7] представлена на Рисунку 1.2.

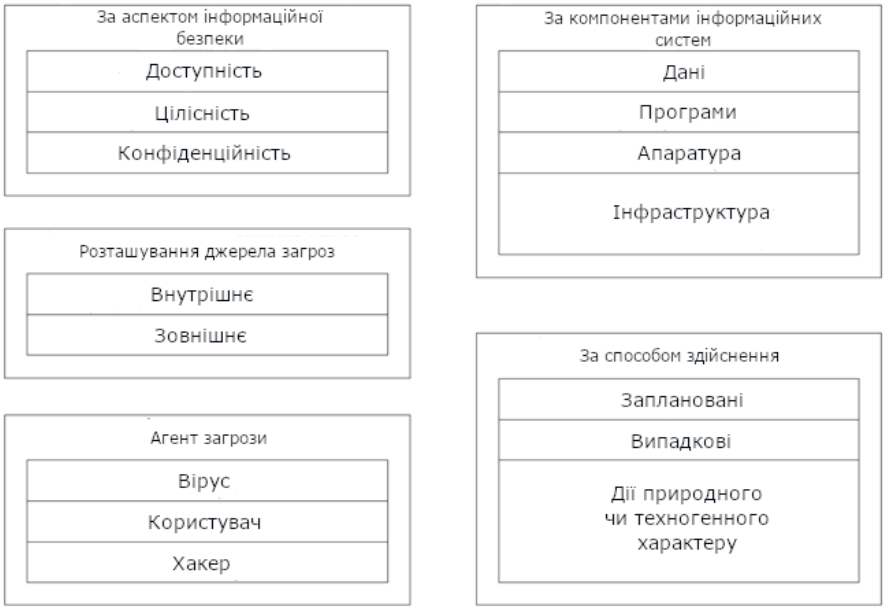

Рисунок 1.2 – Класифікація загроз за критеріями

Далі для дослідження в якості основного буде розглянутий критерій по аспекту інформаційної безпеки (за необхідності розглядаючи інші критерії), а саме загрози доступності, цілісності і конфіденційності даних.

Найбільш поширені загрози доступності – наслідки випадкових помилок. Помилки у програмі або неправильно введені дані, які викликали збій усієї системи. Зазвичай вони залишають уразливості у системі, які може використати зловмисник. Інші загрози доступності АСУ ТП класифікуємо за компонентами АСУ ТП, на які націлені загрози:

– відмова користувачів
– відмова інформаційної системи
– відмова інфраструктури, яка підтримується

У якості загрози відмови користувача виступає людський фактор. Це може бути відсутність відповідної підготовки у спеціаліста або взагалі неможливість прийняття рішення недосвідченим або некваліфікованим спеціалістом.

Джерелами внутрішніх відмов системи є:

– відступ від правил експлуатації
– системні помилки (надмірний об’єм інформації, яка обробляється)
– помилки адміністрування системи
– відмова програмного забезпечення
– втрата даних і пошкодження апаратури (викрадення носіїв інформації, втрата підключення до ліній зв’язку)

У відношенні до інфраструктури, яка підтримується, це може бути частковий або повний вихід з ладу підсистем (порушення роботи мереж зв’язку, електрозабезпечення, системи охоронно-пожежної безпеки).

Для загроз цілісності АСУ ТП потрібен безпосередній фізичний доступ до системи. Потенційно вразливими як дані, так і програми. Дані зловмисник може підмінити маючи безпосередній доступ до системи. Шкідливе ПЗ, у свою чергу, є загрозою пам’яті програм.

Також до загроз цілісності можна віднести втрату інформації при передачі даних через канали зв’язку[8]. Часткова втрата пакетів у мережах телекомунікації

АСУ ТП може призвести до отримання неправильних результатів і до виконання неправильних або непотрібних операцій.

Конфіденційну інформацію в АСУ ТП можна розділити на службову та предметну. Службова інформація (паролі, коди доступу і тд) в АСУ ТП має технічну роль, але порушення її конфіденційності може призвести до несанкціонованого доступу до всієї інформації, у тому числі до предметної.

Перехват даних – дуже серйозна загроза. Якщо конфіденційність даних є одним із ключових завдань при проектування системи, а дані передаються по багатьох каналах зв’зку, то їх захист може виявитись досить складним та вартісним завданням. Існують спеціальні засоби перехвату, за допомогою яких зловмисник може перехватити конфіденційну інформацію. Далі розглянемо таблицю 1.2 у якій представлені основні загрози інформаційної безпеки АСУ ТП.

Таблиця 1.2 – Основні загрози

Способи нанесення шкоди	Об’єкти впливу			
	Обладнання	Програми	Дані	Персонал
Розкриття інформації	Викрадення носіїв інформації, підключення до систем лінії зв’язку, несанкціонований доступ до ресурсів.	Несанкціоноване копіювання даних, перехват.	Викрадення, копіювання, перехват.	Розголошення відомостей про захист АСУ, халатність працівника.
Втрата цілісності інформації	Підключення, модифікація, зміна режимів роботи, несанкціонований доступ до ресурсів.	Упровадження апаратних закладок, вірусів і “троянів”.	Викривлення, модифікація.	Людський фактор (вербування, власна вигода і тд).
Порушення роботоздатності АСУ	Зміна режимів функціонування, вихід з ладу, викрадення.	Викривлення, підміна, видалення.	Викривлення, видалення, неправдиві дані.	Відсутність працівника.

1.6 Уразливості промислових систем

У промислових системах критичної інфраструктури існують ті ж уразливості, що і в більшості звичайних IT систем. Крім цього, особливістю промислових систем є існування унікальних уразливостей, до яких можна віднести:

- людський фактор. Експлуатацією промислових та корпоративних систем зазвичай займаються різні підрозділи та спеціалісти. У свою чергу, персонал промислових систем, як правило, достатньо далекий від питань забезпечення інформаційної безпеки, у його складі немає спеціалістів з безпеки, а рекомендації IT персоналу на нього не розповсюджуються. Вирішення технологічних проблем виникаючих в ході експлуатації системи, забезпечення її надійності і доступності, підвищення ефективності і мінімізація накладних витрат мають бути одними з основних завдань спеціалістів.
- уразливості ОС. Уразливості ОС (операційних систем) властиві як для промислових, так для корпоративних систем, але встановлення програмних корекцій у промислових системах зазвичай не виконується. Безперебійна роботи такої системи є відповідальністю адміністратора. Установлення попередньо не протестованих програмних корекцій може сприяти серйозним проблемам, а на повноцінне тестування немає ні часу, ні грошей.
- аутентифікація. Зазвичай для промислових систем використовують загальні паролі. Система двофакторної аутентифікації використовується дуже рідко, а конфіденційна інформація часто передається у відкритому вигляді.
- віддалений доступ. Для управління промисловими системами досить часто використовується віддалений доступ по комутованих каналах або по VPN каналах через мережу Інтернет. При неправильному та не

контрольованому використанні це може призвести до серйозних проблем з безпекою.

- зовнішні мережеві підключення. Відсутність відповідної нормативної бази і використання спрямоване у більшій мірі на зручність, а не безпеку, деколи призводять до того, що між промисловими та корпоративними мережами створюються мережеві підключення. Існують навіть рекомендації з використання “комбінованих” мереж, які дозволяють спростити адміністрування. Це може негативно вплинути на безпеку як і промислової, так і корпоративної систем.
- засоби захисту та моніторингу. На відміну від корпоративних систем, використання IDS. Антивірусів тощо у промислових системах не є розповсюдженою практикою, також не рідко обходять стороною аналіз журналів аудиту безпеки.
- бездротові мережі. У промислових системах часто використовують різні види бездротового зв’язку, включаючи протоколи 802.11, які, як відомо, не надають достатніх можливостей з захисту інформації.
- віддалені процесори. Деякі класи віддалених процесорів мають відомі вразливості. Продуктивність цих процесорів не завжди дозволяє реалізувати функції безпеки. Крім того, після встановлення їх стараються не чіпати роками, протягом яких вони залишаються уразливими.
- програмне забезпечення. Програмне забезпечення промислових систем зазвичай не має достатньої кількості безпекових функцій. Крім того, у більшості випадків, воно не позбавлене архітектурних слабкостей.
- розкриття інформації. Нерідко власники промислових систем свідомо публікують інформацію про їх архітектуру. Консультанти та розробники часто діляться досвідом та розкривають корисну для зловмисників інформацію про працівників.
- фізична безпека. Віддалені процесори та устаткування промислових систем можуть знаходитись за межами контрольованої зони. У таких

умовах вони фізично не можуть контролюватись персоналом, і єдиним механізмом їх фізичного захисту є використання металевих дверей і замків. Такі заходи не є серйозною перешкодою для зловмисників.

Таким чином можна зробити висновок, що існує значна кількість вразливостей, які є як загальними для будь-яких інформаційних систем, так і специфічними для промислових систем. Ці вразливості зумовлюють особливі вимоги до безпеки та особливі режими експлуатації таких систем.

Висновки до розділу 1

У першому розділі був проведений аналіз структури АСУ ТП, описані основні компоненти системи. Можна зробити висновок, що при проектуванні АСУ ТП, необхідно ознайомитись зі всіма потребами контрольованого об’єкту. Побудова мережі верхнього рівня, вибір компонентів, реалізація взаємодії обладнання на нижньому рівні – на всі ці питання потрібно дати відповідь ще до початку проектування.

Досліджені основні загрози інформаційній безпеці АСУ ТП. Створена таблиця основних загроз ІБ у АСУ ТП та були виявлені основні способи нанесення шкоди.

Досліджені основні вразливості, які властиві сучасним промисловим системам.

2 БЕЗПЕКА В АСУ ТП

2.1 Загальні відомості

Не дивлячись на кількість аварій з катастрофічними наслідками, проблема безпеки автоматизованих систем управління технологічними процесам на підприємствах хімічної та не тільки промисловості ніколи не стояла так гостро як останніми роками.

Загальний інтерес до безпеки промислових систем виник лише після інцидентів з комп'ютерними вірусами Stuxnet, Duqu, Flame, які акатували іранські атомні об'єкти, державні заклади та промислові об'єкти Індії, Китаю та інших країн. До появи цих інцидентів вважалось, що скомпрометувати роботу АСУ ТП було дуже важко. Такі уявлення будувались на наступних постулатах: програмне забезпечення кожної АСУ ТП унікальне і закрите; проникнення в АСУ ТП пов'язане з великими витратами інтелектуальних ресурсів, а грошова винагорода для зловмисника не очевидна; локальна мережа АСУ ТП вирішує проблеми обмеження доступу.

Вивчення структури та програмно-апаратних засобів, що використовуються в АСУ ТП, показало, що за останній час пройшли великі зміни. Майже всюди використовується широко розповсюджене програмне забезпечення (ПЗ) як ОС Windows, TCP/IP протоколи і тд, які разом зі своїми перевагами з стандартності, простоті та якості використання принесли також і недоліки – вразливості. Також нерідко у мережі АСУ ТП з'являються комп'ютери, підключені до мережі Інтернет, що також вносить велику кількість потенційних загроз до системи.

Атаки на промислові системи часто здійснюються за допомогою програмних засобів, розроблених не тільки окремими хакерами (зовнішніми, а часто внутрішніми користувачами систем), а й організованими групами висококваліфікованих спеціалістів. Так, спеціалісти, які аналізували Stuxnet відмічають, що цей вірус мав цільовий код, який задовольняв цілий ряд специфічних потреб та реалізував повноцінну атаку на системи АСУ ТП виробництва саме компанії Siemens. Також для реалізації потенціалу нападу,

вірусу були необхідні частотні перетворювачі виробництва двох компаній: Vacon (Фінляндія) та Fararo Paya (Іран), працюючих на частотах від 120 до 807Гц. Наявність подібних вимог дозволило більшості експертів, які досліджували цей код, зробити висновок про те, що вірус призначався для точкової атаки цілком визначеної групи виробництв. Згідно з аналізом, проведеним спеціалістами компанії Symantec, шкідливий код Stuxnet реалізував атаку зразу на кількох рівнях: на рівні операційної системи Windows, ПЗ управління АСУ ТП Siemens WinCC/PCS 7 і безпосередньо програмованих логічних контролерів Siemens S7-300, які обслуговували перетворювачі частот (які, у свою чергу, керували швидкістю обертання електродвигунів).

За даними компанії Siemens, з 15 випадків зараження вірусом у Німеччині, у жодному з випадків не було проникнення до програмованих логічних контролерів у той час як на іранських об’єктах це виявилось можливо. Таким чином, атака була добре підготована спеціалістами, які мали досить значні знання про об’єкти атаки. Це дозволяє зробити висновок, що атака була проведена групою професіоналів, а зловмисниками-одинаками.

Також недавно з’явився новий термін “кібервійна” (cyberwarfare), який часто згадується у засобах масової інформації у зв’язку з проблемою захисту систем АСУ ТП на інфраструктурних об’єктах та небезпечних виробництвах. У багатьох країнах створені спеціалізовані підрозділи для виведення з ладу інфраструктури та виробництва у ворожих країнах. Прикладом роботи такого підрозділу було виведення системи радіолокаційного визначення повітряних цілей в Іраку.

Таким чином повсюдне використання комп’ютерного обладнання у керування промисловими підприємствами створює необхідність все більшої і більшої уваги до проблем інформаційної безпеки (ІБ) таких систем.

Огляд стану безпеки АСУ ТП, проведений компанією Positive Technologies у 2017 році показав досить тривожну картину: спостерігається збільшення кількості вразливостей. З 2015 по 2017 роки встановлено у 20 разів більше вразливостей ніж за останні 5 років. Кожна п’ята вразливість знешкоджується

більше місяця. Більше половини вразливостей дозволяють хакерам запускати програмний код, що теоретично надає повний доступ до системи.

Основні проблеми інформаційної безпеки АСУ ТП, які виділяють експерти, з'являються через:

- слабкий захист від несанкціонованого доступу (паролі)
- недекларованих можливостей SCADA
- відсутність контролю керуючих впливів
- використання бездротових комунікацій (некрипостійке шифрування Wi-Fi)
- відсутність чітких меж між різними сегментами мережі
- несвоєчасне чи некоректне оновлення програмного забезпечення
- Web-технології, які використовуються на верхньому рівні АСУ ТП
- відмову від навіть мінімальних заходів безпеки (нерідко заради зручності чи продуктивності, компанії відмовляються від встановлення не тільки, наприклад, антивірусного захисту, а навіть захисту паролем критично важливих активів)
- поширення Windows як операційної системи для робочих станцій та навіть серверів
- розробку з розрахунком на використання у довіреному середовищі закритих індустріальних мереж
- створення систем без врахування кращих практик розробки безпечного коду
- людський фактор, слабку дисципліну персоналу

Типова АСУ ТП має від двох до трьох рівнів мережевої архітектури. На сучасних підприємствах все частіше реалізується єдине середовище керування у корпоративній ЛОМ (локальній обчислювальній мережі), в якій розміщені комп'ютери та системи, за допомогою яких відбувається керування організаційною та фінансовою діяльністю. Частина комп'ютерів цієї мережі може мати доступ до серверів АСУ ТП, які мають інформацію про технологічний процес.

Мережа АСУ ТП може мати і верхній рівень (станції операторів і інженерів системи, сервери баз даних, сервери програм), і нижній рівень (давачі збору даних і виконавчі механізми). Зв'язок між ними забезпечується комунікаційними серверами та контролерами. Доступ до давачів здійснюється за допомогою протоколів на польових шин (RS485, RS232, Fieldbus, ProfiBus, CAN, OPC та інших).

Сучасною тенденцією є використання IP та Ethernet мереж на високому та середньому рівнях. Усе частіше промислові пристрої мають Ethernet порти та IP протоколи, які використовуються на всіх рівнях АСУ ТП.

Таким чином, особливістю мереж АСУ ТП є використання разом з IP ще й додаткових спеціалізованих протоколів, які якщо і ускладнюють проникнення у системи, то, як показують інциденти, недостатньо, щоб запобігти атаки професіоналів.

Наведемо приклад основних загроз АСУ ТП, знайдених після аналізу справжніх інцидентів:

- атаки на SCADA
- атаки на ПЛК, вразливості ПЛК (стандартний пароль, неавторизований доступ до оригінального програмного забезпечення)
- атаки на інфраструктуру та оперативну систему (віруси, троянські програми, черв'яки, DoS- і DDoS-атаки, ARP-спуфінг – перехват трафіку пілся оголошення себе маршрутизатором)
- атаки на протоколи, вразливість протоколів (несанкціонований доступ, SQL-ін'єкції)
- практичні атаки (переповнення буферу – Buffer Overflow, розкриття інформації – Information Disclose, відмова в доступі – Denial of Access, підміна представлення – Manipulation of View)

Серед усіх типів вразливих компонентів АСУ ТП переважають SCADA – 87%, системи, які забезпечують інтерфейси людина-машина – 49%, програмовані контролери – 20%, протоколи – 1%.

Доля вразливостей по типах розділилась наступним чином: переповнення

буферу – 36%, аутентифікація/управління ключами – 22.86%, вразливості Web-програм – сервер – 10.86%, клієнт – 9.14%, віддалене виконання коду – 13.14%.

Унаслідок експлуатації АСУ ТП (розробка та експлуатація можуть складати більше 10 років) і суттєвої зміни складу і якості сучасних загроз, необхідно проектувати і реалізовувати інформаційну безпеку систем з врахуванням тенденцій розвитку кіберзагроз. З іншого боку необхідно проводити регулярну роботу з нейтралізації виникаючих чи потенційних загроз на працюючих системах.

Сукупність нейтралізуючих заходів можна розділити на дві групи: адміністративно-організаційні та програмно-технічні.

Перша група заходів пов’язана з формуванням програми робіт з забезпечення ІБ АСУ ТП і розробкою документів, які регламентують високорівневий підхід до забезпечення ІБ, а також описують політику розвитку системи ІБ АСУ ТП. Крім того формується пакет організаційної документації, направленої на створення і підтримку режиму ІБ АСУ ТП.

Програмно-технічні заходи створюють основний набір засобів забезпечення ІБ АСУ ТП. На цьому рівні реалізуються наступні сервіси ІБ: управління доступом, забезпечення цілісності, забезпечення безпечного міжмережевої взаємодії, антивірусний захист, аналіз захищеності, виявлення вторгнень, управління системою ІБ (неперервний моніторинг стани, виявлення інцидентів, реагування). Конкретні вимоги до перелічених сервісів представляються на основі аналізу інформації, яка обробляється, та оцінки загроз безпеки АСУ ТП.

Кожна група засобів у залежності від необхідності і можливостей підприємства може використовуватись на одному з трьох рівнів. Базовий рівень включає механізми, традиційні для більшості інформаційних систем. Середній рівень передбачає виконання початкових тактичних заходів, які забезпечують реалізацію керуючих захисних функцій з забезпечення ІБ. На розширеному (високому) рівні реалізуються заходи, які підтримують і розширюють базовий та середній рівні, але для їх впровадження може бути потрібна додаткова експертиза.

Так, для першої групи заходів на базовому рівні передбачається розробка

документів, які описують політику кібербезпеки, впровадження політик та процедур з державних стандартів безпеки критично важливих об’єктів. На середньому рівні ведуться роботи з впровадження найкращих індустріальних практик, здійснюється контроль виконання політик та процедур. На розширеному рівні впроваджується процес неперервного покращення політик та процедур ІБ, періодично проводяться навчання та аудит. Для ілюстрації різних рівнів другої групи заходів розглянемо сервіс забезпечення безпечної міжмережевої взаємодії.

На базовому рівні потрібне впровадження електронного периметру та відключення всіх необов’язкових для основного процесу з’єднань. Створюється та оновлюється список критичних об’єктів. На середньому рівні електронний периметр розділяється на зони: ЛОМ АСУ ТП, демілітаризована зона та зона корпоративної ЛОМ. Аналізується та мінімізується кількість ресурсів, одночасно доступних з мережі АСУ ТП та корпоративної ЛОМ. Постачальники обладнання та інтегратори періодично проводять навчання працівників.

2.2 Математична модель впливу загроз на ІС

У цьому розділі запропонована математична модель впливу внутрішніх та зовнішніх загроз на інформаційну систему обробки персональних даних. Поетапно розписаний процес побудови двох математичних моделей інформаційної системи: з допомогою ланцюга Маркова з неперервним часом, з допомогою ланцюга Маркова з дискретними моментами переходу з одного стану в інший. Запропонована методика знаходження актуальних загроз безпеці даних при їх обробці. Наведені приклади розрахунків імовірностей знаходження математичної моделі інформаційної системи в одному з чотирьох станів (загроза не надійшла; загроза надійшла, але не була реалізована; загроза надійшла, була реалізована; загроза надійшла, але була відбита системою захисту)[8].

Систему можна інтерпретувати як систему масового обслуговування, в яку надходять загрози. Для початку розглянемо ситуацію, коли на вхід до системи надходять загрози одного типу, припускаючи, що загроза не може бути

реалізована та надходити кілька разів в один і той же період часу. Якщо умови вище виконуються, то система може знаходитись у одному з чотирьох станів (Рисунок 2.1):

1. Загроза не надходила і, відповідно, не була реалізована
2. Загроза надійшла, але не була реалізована
3. Загроза надійшла та була реалізована
4. Загроза надійшла, але була відбита системою захисту

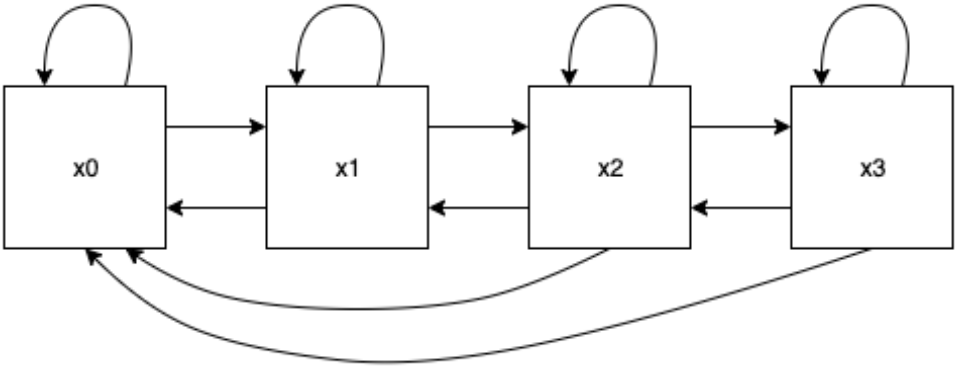

Рисунок 2.1 – Граф станів системи

Система, яка розглядається є системою з відновленням, тобто система може переходити з будь-якого стану в початковий. Будемо розглядати систему з неперервним часом. Перехід зі стану у стан відбувається згідно орієнтованого графу, дивись рисунок 2.1. Для опису процесу переходу зі стану у стан, побудуємо матрицю інтенсивностей переходу[9]:

$$p_{ij} = \begin{vmatrix} \lambda_{11} & \lambda_{12} & \lambda_{13} & 0 \\ \lambda_{21} & \lambda_{22} & \lambda_{23} & \lambda_{24} \\ \lambda_{31} & \lambda_{32} & \lambda_{33} & \lambda_{34} \\ \lambda_{41} & \lambda_{42} & \lambda_{43} & \lambda_{44} \end{vmatrix} \quad (2.1)$$

З попередніх погоджень випливає, що елементи цієї матриці мають такі властивості:

$$\begin{aligned}\lambda_{11} &= -\lambda_{12} - \lambda_{13}\\ \lambda_{22} &= -\lambda_{21} - \lambda_{23} - \lambda_{24}\\ \lambda_{33} &= -\lambda_{31} - \lambda_{32} - \lambda_{34}\\ \lambda_{44} &= -\lambda_{41} - \lambda_{42} - \lambda_{43}\end{aligned} \quad (2.2)$$

Елементи матриці інтенсивностей можуть бути обраховані за допомогою імітаційної моделі, запропонованої в [6]. У цій роботі опишемо імовірнісно-аналітичний спосіб їх визначення. Для визначення імовірностей перебування системи у станах x_0, x_1, x_2, x_3, побудуємо систему диференційних рівнянь:

$$\begin{cases}\dfrac{dp_0(t)}{dt} = p_0(t)\lambda_{11} + p_1(t)\lambda_{21} + p_2(t)\lambda_{31} + p_3(t)\lambda_{41}\\ \dfrac{dp_1(t)}{dt} = p_0(t)\lambda_{12} + p_1(t)\lambda_{22} + p_2(t)\lambda_{32} + p_3(t)\lambda_{42}\\ \dfrac{dp_2(t)}{dt} = p_0(t)\lambda_{13} + p_1(t)\lambda_{23} + p_2(t)\lambda_{33} + p_3(t)\lambda_{43}\\ \dfrac{dp_3(t)}{dt} = p_1(t)\lambda_{24} + p_2(t)\lambda_{34} + p_3(t)\lambda_{44}\end{cases} \quad (2.3)$$

Так, як

$$p(0) = (1,0,0,0) \quad (2.4)$$

заданий, то вектор абсолютних імовірностей[10]:

$$p(n) = (p_0(n), p_1(n), p_2(n), p_3(n)) \quad (2.5)$$

визначається відношенням:

$$p(n) = p(0)\left\|p_{ij}(n)\right\| \quad (2.6)$$

Після проведення дослідження було визначено два результати знаходження коефіцієнтів λ_{ij}, які будуть наведені нижче (розділ 2.2.1 та розділ 2.2.2).

2.2.1 Приклад числової реалізації моделі

Отримавши коефіцієнти λ_{ij}:

$$\begin{vmatrix} -0.040 & 0.015 & 0.010 & 0.015 \\ 0.225 & -0.250 & -0.025 & 0.050 \\ 0.625 & -0.160 & -0.855 & 0.390 \\ -0.000 & 0.075 & 0.200 & -0.275 \end{vmatrix} \quad (2.7)$$

побудуємо розв’язок завдання методом Рунге-Кутти четвертого порядку для моменту часу $t = 50$с. У результаті проведених обчислень були знайдені значення імовірності знаходження системи у кожному зі станів, які представлені в таблиці 2.1.

Таблиця 2.1 – Результати обчислень.

Значення часу, t	Імовірність знаходження у стані x_0	Імовірність знаходження у стані x_1	Імовірність знаходження у стані x_2	Імовірність знаходження у стані x_3
1	0.9649	0.0129	0.0075	0.0147
2	0.9372	0.0227	0.0123	0.0279
3	0.9149	0.0302	0.0156	0.0393
…	…	…	…	…
25	0.8132	0.0584	0.0306	0.0978
…	…	…	…	…
50	0.8119	0.0586	0.0309	0.0987

Перенісши отримані значення імовірностей на графік, отримаємо такий результат:

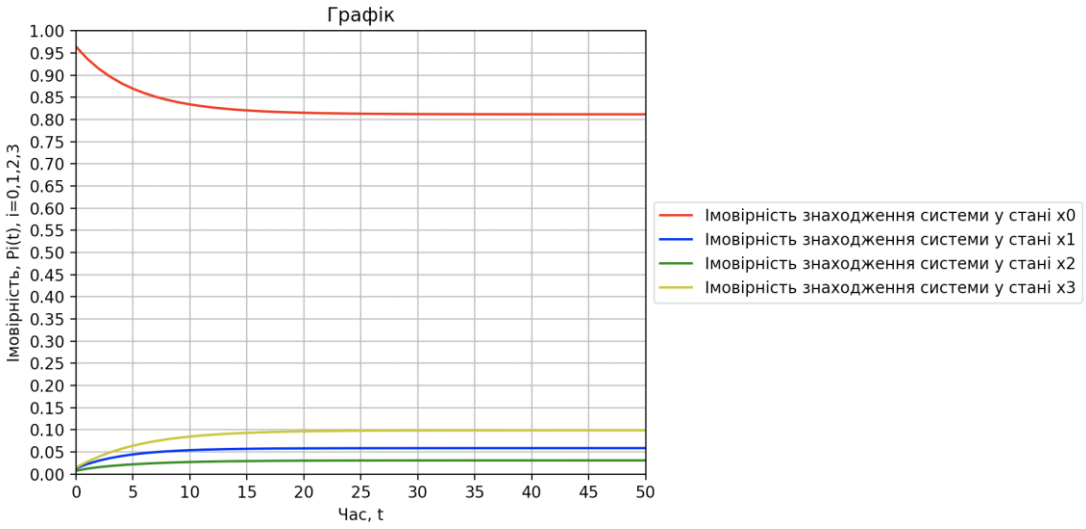

Рисунок 2.2 – Імовірність знаходження системи у кожному зі станів

2.2.2 Приклад числової реалізації моделі

Зробимо аналогічні до попереднього прикладу обчислення, результати у таблиці 2.2, λ_{ij}:

$$\begin{vmatrix} -0.040 & 0.015 & 0.010 & 0.015 \\ 0.225 & -0.250 & -0.025 & 0.050 \\ 0.575 & -0.200 & -0.875 & 0.500 \\ -0.125 & 0.145 & 0.180 & -0.200 \end{vmatrix} \quad (2.8)$$

Таблиця 2.2 – Результати обчислень.

Значення часу, t	Імовірність знаходження у стані x_0	Імовірність знаходження у стані x_1	Імовірність знаходження у стані x_2	Імовірність знаходження у стані x_3
1	0.9637	0.0133	0.0074	0.0156
2	0.9328	0.0242	0.0120	0.0310
3	0.9057	0.0335	0.0153	0.0455
…	…	…	…	…
25	0.6859	0.1051	0.0394	0.1696
…	…	…	…	…
50	0.6650	0.1116	0.0418	0.1817

У результаті отримаємо такий графік:

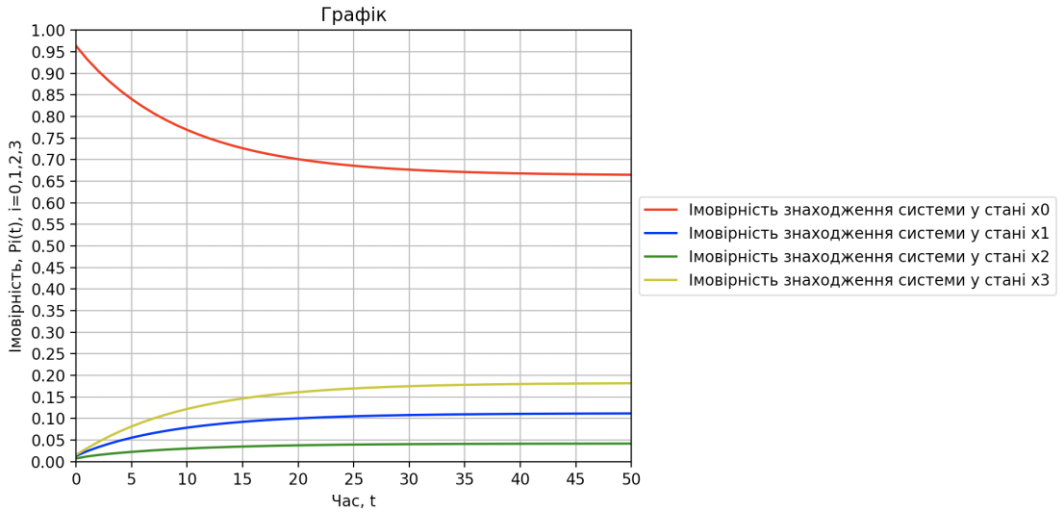

Рисунок 2.3 – Імовірність знаходження системи у кожному з станів

Висновки до розділу 2

На основі отриманих результатів можна сказати, що у варіанті 2 більша імовірність знаходження системи у стані, який викликаний отриманням загрози, хоча також велика вірогідність успішного відбиття загрози системою захисту.

Запропонована математична модель реалізації загроз безпеки інформаційної системи. Також розроблена та представлена на основі цієї моделі методика виявлення актуальних загроз безпеки.

Приклади числових результатів аналізу за допомогою запропонованої методики наочно показують, що їх використання допомагає з виділенням загрози, які є актуальними для досліджуваної системи та можуть використовуватись на практиці. Недоліком запропонованої методики є необхідність розгляду поведінки системи при дії на неї кожного типу загроз окремо і неможливість визначення поведінки про одночасній дії кількох загроз. Але з іншого боку вивчення впливу кожної загрози окремо дозволяє більш детально вивчити кожен її тип та виділити ті, вірогідність появи яких є найбільшою.

3 УПРАВЛІННЯ АСУ ТП З ВРАХУВАННЯМ БЕЗПЕКИ

Базове функціонування будь-якої АСУ ТП зображене на Рисунку 3.1. Але критичні процеси повинні також включати додаткові системи безпеки. Типова АСУ ТП має численні цикли контролю, інтерфейси людина-машина (ЛМІ) та віддалені діагностики та підтримки. Цикл контролю використовує давачі, виконавці та контролери для керування технологічним процесом. Давач – це пристрій, який виконує вимірювання деякої фізичної величини та надсилає результат у контролер. Контролер обробляє сигнали та генерує відповідні сигнали управління, засновуючись на раніше заданому алгоритмі. Виконавці такі як клапани, перемикачі та мотори маніпулюють технологічним процесом під впливом команд з контролера.

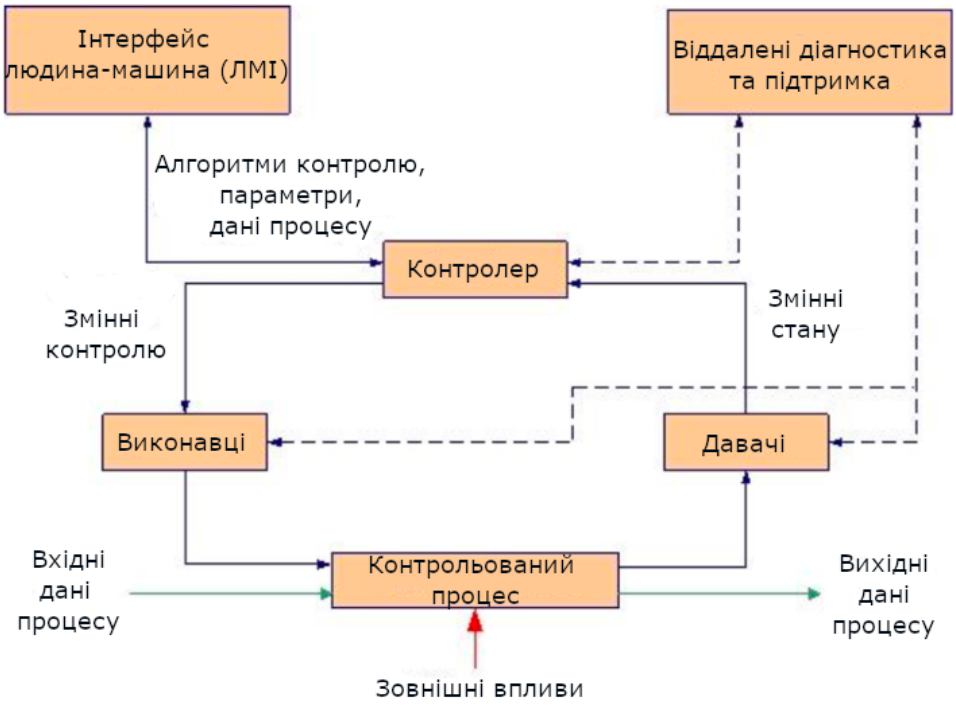

Рисунок 3.1 - Функціонування АСУ ТП

Типова АСУ ТП (Рисунок 3.2) містить численні контури управління, інтерфейси користувача, а також засоби віддаленої діагностики та обслуговування, побудовані з використанням багатьох мережевих протоколів на архітектурах багатошарових мереж. Цикл управління використовує давачі, виконавчі пристрої та контролери для управління деяким контрольованим процесом. Давач - це пристрій, який виробляє вимірювання деякої фізичної властивості і потім посилає цю інформацію як контрольовані змінні до контролера. Контролер інтерпретує сигнали і генерує відповідні маніпульовані змінні, засновані на алгоритмі управління і цільових заданих точках, які він передає на виконавчі механізми. Приводи, такі як регулюючі клапани, вимикачі, перемикачі та двигуни, використовуються для безпосереднього керування контрольованим процесом на основі команд від контролера.

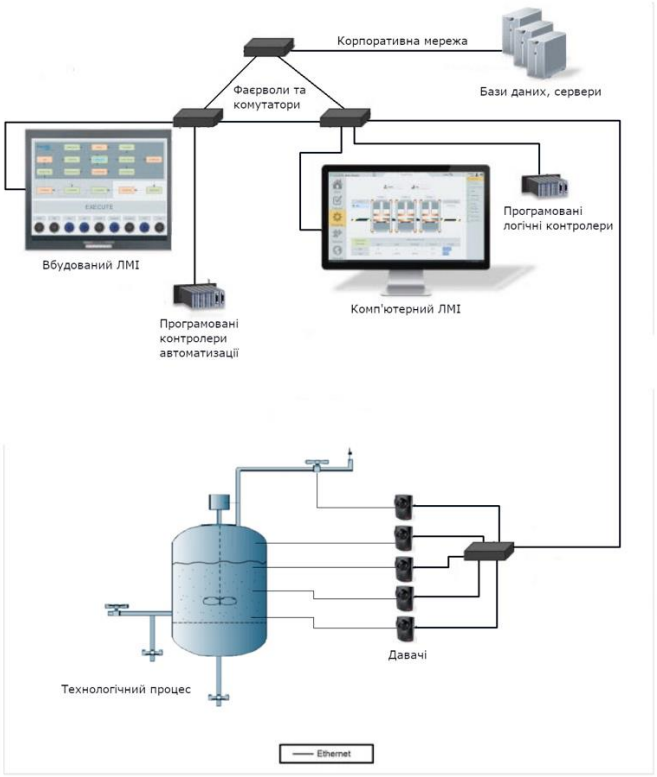

Рисунок 3.2 – Структура типової АСУ ТП

Дуже часто для моделювання систем контролю за розподіленими даними, де дуже важливе їх централізоване відображення та керування. Для моделювання таких систем використовують SCADA-програми. Прикладами таких систем є системи розподілу водних ресурсів, транспортування нафти та природного газу, електроенергії тощо (Рисунок 3.3).

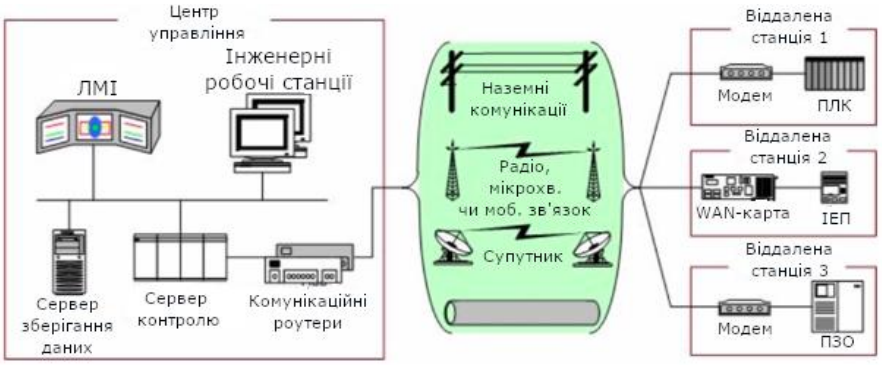

Рисунок 3.3 - Типова схема SCADA-системи

SCADA-системи інтегрують системи збору даних з системами передачі даних та програмне забезпечення ЛМІ для забезпечення централізованої системи моніторингу та управління для численних технологічних входів і виходів. Вони призначені для збору польової інформації, передачі її на центральний комп'ютерний комп'ютер і відображення інформації оператору графічно або текстово, що дозволяє оператору контролювати або керувати цілою системою з центрального розташування в режимі реального часу. На підставі складності та налаштування індивідуальної системи, управління будь-якою окремою системою, операцією або завданням може бути автоматичним, або може виконуватися командами оператора.

Рисунок 3.4 показує приклад реалізації SCADA-системи. Вона складається з первинного центру управління і трьох ділянок. Другий резервний контрольний центр забезпечує надмірність у випадку несправності основного центру керування. Підключення "точка-точка" використовуються для всіх центрів керування для зв'язку на місцях, з двома з'єднаннями з використанням радіотелеметрії. Третє поле є локальним для центру управління і використовує

WAN для зв'язку. Обласний центр управління знаходиться над первинним контрольним центром для більш високого рівня контролю. Корпоративна мережа має доступ до всіх центрів керування через глобальну мережу, і доступ до місцевих ділянок здійснюється дистанційно для усунення несправностей та операцій з обслуговування. Головний центр управління опрацьовує польові пристрої для даних через певні проміжки часу (наприклад, 5 секунд, 60 секунд) і може посилати нові задані точки на польовий пристрій відповідно до вимог. На додаток до опитування та видачі команд високого рівня, сервер керування також спостерігає за пріоритетними перериваннями, що надходять з систем сигналізації на місцях.

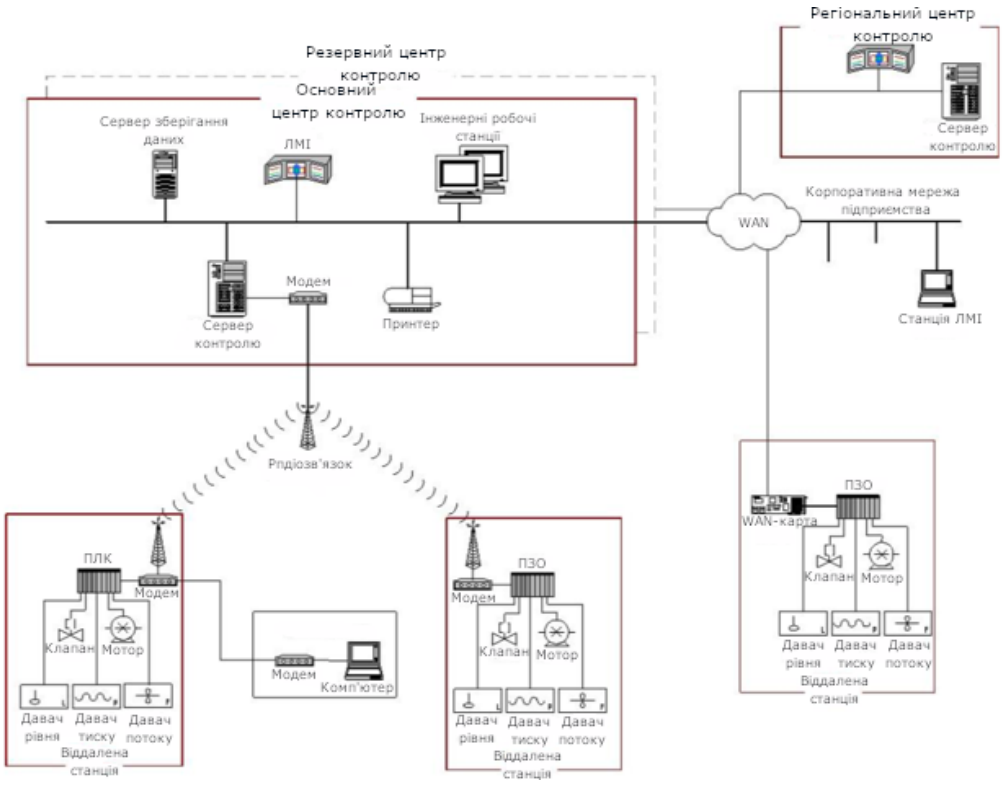

Рисунок 3.4 - Приклад реалізації SCADA-системи

На Рисунку 3.5 показаний інший приклад реалізації для моніторингу та контролю. Цей приклад включає в себе центр управління, в якому знаходиться SCADA-система і три секції системи. Система SCADA опрацьовує інформацію з секцій, наприклад, про стан сигнальних систем, систем електрифікації та інших. Ця інформація також відображається на консолі оператора на станції ЛМІ в центрі

управління. Система також здійснює моніторинг вхідних даних оператора в центрі управління і розподіляє команди високого рівня по виконавчих секціях. Крім того, система SCADA здійснює моніторинг умов на окремих ділянках системи та видає команди на основі цих умов.

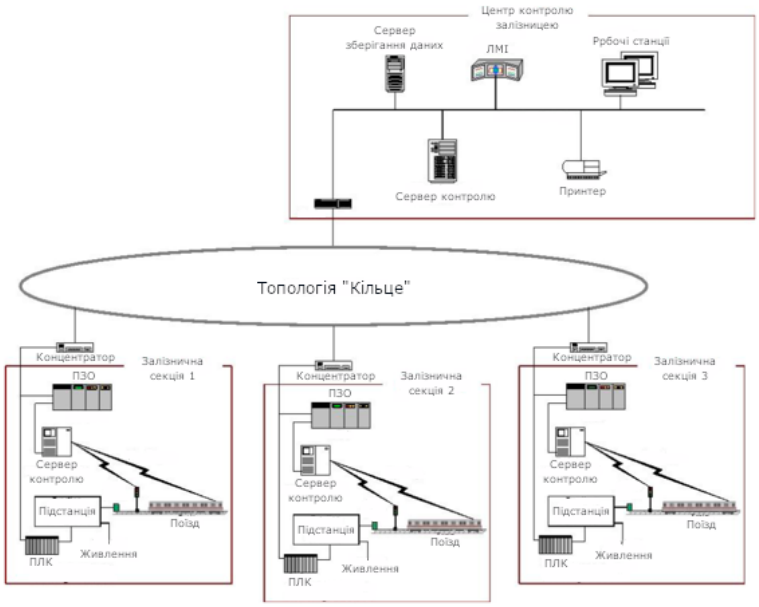

Рисунок 3.5 – Приклад реалізації SCADA-системи

Розподілені системи контролю (РСК) використовуються для управління виробничими системами в межах одного географічного розташування для таких галузей, як нафтопереробні заводи, водопостачання та очищення стічних вод, електростанції, хімічні виробничі підприємства, автомобілебудування та фармацевтичні підприємства. Ці системи зазвичай є системами керування процесами або дискретними системами управління частинами.

Приклад реалізації, що показує компоненти та загальну конфігурацію РСК, зображений на Рисунку 3.6. РСК охоплює весь комплекс від виробничих процесів нижнього рівня до корпоративного або корпоративного рівня. У цьому прикладі контрольний контролер (контрольний сервер) здійснює зв'язок з підлеглими через мережу управління. Керівник надсилає задані точки та запитує дані від розподілених контролерів поля. Розподілені контролери керують своїми

виконавчими пристроями на основі команд керуючого сервера та датчика зворотного зв'язку від датчиків процесу.

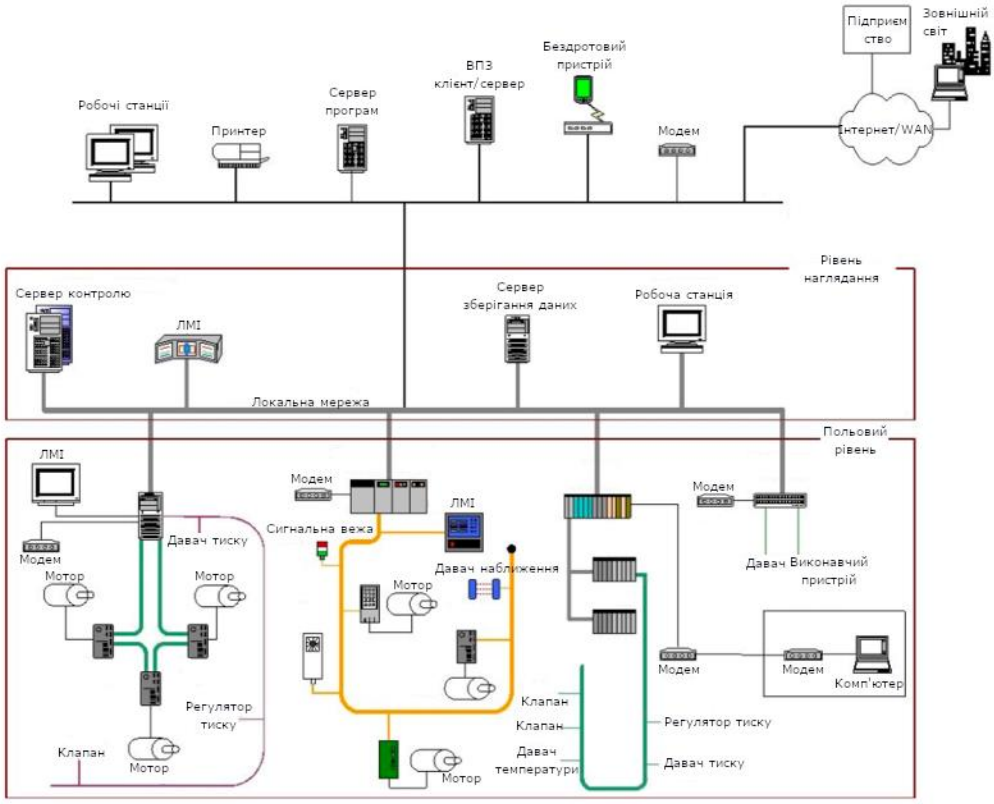

Рисунок 3.6 – Приклад розподіленої системи контролю

На Рисунку 3.6 наведено приклади контролерів низького рівня, знайдених у РСК. Показані пристрої контролю поля включають в себе ПЛК, контролер процесу, контролер одного циклу і контролер машини. Контролер з однією петлею з'єднує датчики та виконавчі пристрої за допомогою проводки "точка-точка", в той час як інші три польові пристрої включають мережі польових шин для взаємодії з датчиками процесу та виконавчими пристроями. Мережі польових шин виключають необхідність прокладки між точками в точці між контролером і окремими давачами та приводами.

Забезпечення безпеки засноване на комбінації ефективних політик безпеки та правильно налаштованої сукупності протоколів безпеки. Вибір, розробка та впровадження протоколів безпеки АСУ ТП може мати значний вплив на функціонування системи, тому критично важливо враховувати:

– які засоби безпеки потрібні, щоб адекватно перенести ризики на допустимий рівень, який не заважає функціонуванню бізнес-функцій системи?
– чи були обрані заходи безпеки впровадження раніше та чи є план їх впровадження?
– який потрібний рівень тестування, щоб перевірити чи заходи безпеки були впроваджені правильно, працюють як потрібно та видають правильний результат?

Ці питання повинні отримати відповідь у контексті ефективного, всеорганізаційного процесу управління ризиками та стратегії кібербезпеки, що знаходить, зменшує та постійно слідкує за ризиками для АСУ ТП.

Ефективна стратегія кібербезпеки АСУ ТП повинна використовувати захист в глибину – техніку розташування механізмів безпеки шарами, коли вплив чи поломка будь-якого механізму має незначний або зовсім не має впливу на інші механізми безпеки. Ця стратегія включає брандмауери, використання демілітаризованих зон і можливості виявлення вторгнень на всій архітектурі АСУ ТП. Використання декількох демілітаризованих зон на Рисунку 3.2 надає додаткову можливість розділяти функціональні можливості та привілеї доступу і виявилося дуже ефективним у захисті великих архітектур, що складаються з мереж з різними оперативними мандатами. Розгортання виявлення вторгнень застосовують різні набори правил і підписи, унікальні для кожного домену, який контролюється.

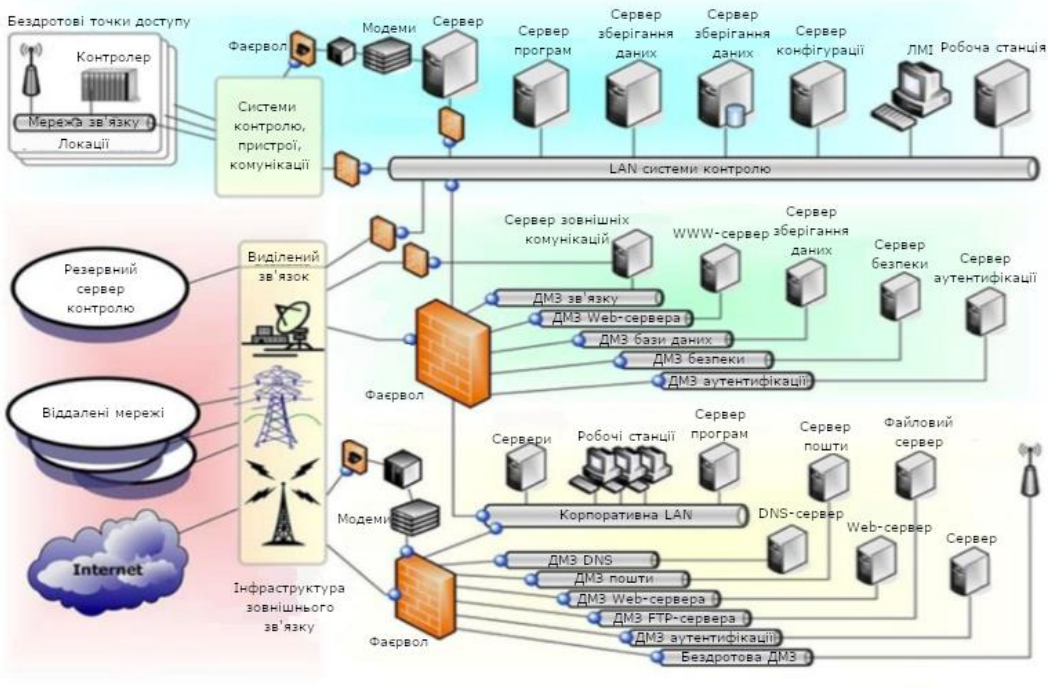

Рисунок 3.7 – Рекомендована архітектура захисту в глибину

3.1 Вибір засобів безпеки

Перед початком вибору засобів безпеки потрібно зібрати інформацію про інформаційну систему у векторі потенційних збитків про аварії. Для будь-якої інформаційної системи можна виділити 3 властивості – конфіденційність, цілісність, доступність – які асоційовані з одним з трьох рівнів потенційного впливу. Також важливо пам’ятати, що для АСУ ТП, доступність вважається найважливішою.

Базові заходи є початковим пунктом для обрання заходів безпеки та обираються на основі категорії безпеки та співставляються з ризиком та впливами при аварії дослідженими раніше.

Для того, щоб скористатися розширеним списком заходів безпеки та захисту інформації і для того, щоб дати організаціям більшу гнучкість та спритність у захисті їх інформаційних систем, був введений концепт шарів. Шари надають структурований підхід, щоб допомогти організаціям розширити свій захист базових ресурсів та розробити плани захисту кожної окремої функції АСУ

ТП. Шар – це повний набір заходів безпеки, покращення контролю та додаткових керівництв.

У загальному, шари призначені для зменшення потреби в у загальних засобах безпеки, а використанні лише тих, які краще підходять у певних ситуаціях, умовах та обставинах. Але шари ніяк не виключають використання загальних, всеорганізаційних політик безпеки на будь-яких рівнях. Підхід спеціалізації на кожному окремому підпроцесі є дуже важливим для збільшення захисту всієї системи в цілому та переведення більшості чи всіх показників захищеності з допустимий рівень.

Також потрібно пам’ятати, що будь-яка розробка спеціалізованих заходів безпеки повинна відповідати вимогам та обмеженням всієї системи в цілому. Для прикладу, будь-яка АСУ ТП має вимоги швидкодії, надійності і тд. Якщо впровадження деяких безпекових ініціатив буде погіршувати роботу інформаційної системи у цих показниках, організація має надати повне та раціональне пояснення того, що на даний момент для неї зараз важливіше та повинне бути впроваджене. Такі рішення можуть пізніше змінитись.

3.2 Заходи безпеки для АСУ ТП

Так, як теперішні АСУ ТП є часто комбінацією сучасних систем, систем, які вже працюють від 20 років до 30 років, систем-гібридів, які по суті є старими системами з новим технічним забезпеченням, буває важко впровадити заходи безпеки, слідуючи одному й тому ж самому алгоритму дій. Упровадження заходів безпеки у кожному з цих видів має деякі концептуальні відмінності.

Для нових систем, процес вибору заходів безпеки починається з визначення тільки базових вимог до безпеки, так як система ще не існує та організація може лише здогадуватись про всі можливі впливи на безпеку АСУ ТП. Визначені заходи безпеки для інформаційної системи слугують як загальна специфікація безпеки системи та мають стати основою безпекової політики системи та розширюватись пізніше[12].

Для вже існуючих систем та систем-гібридів, на відміну від систем у розробці, велика ймовірність, що визначення небезпек, категоризація загроз та їх впливів вже були проведені та розробка заходів безпеки вже починається з попередньо узгоджених домовленостей та перспективного бачення розвитку системи[13].

Заходи безпеки поділяються на 18 груп, кожна з груп включає заходи безпеки, які пов’язані з загальною її темою. Контроль безпеки може включати аспекти нагляду за ручними процесами, діями працівників, автономними механізмами. Нижче наведені всі 18 груп, пов’язаних з безпекою:

- контроль доступу. Це процес надання або відхилення конкретних запитів на отримання та використання інформації та пов'язаних з нею послуг з обробки інформації для фізичного доступу до даних в середовищі інформаційної системи.
- обізнаність та тренування. Політики та процедури для забезпечення того, щоб всім користувачам інформаційної системи було надано відповідне навчання з питань безпеки щодо їх використання в системі та збереження точних записів про навчання.
- аудит та підзвітність. Незалежний огляд та експертиза записів та заходів для оцінки адекватності системного контролю, забезпечення дотримання встановленої політики та оперативних процедур, а також рекомендації щодо необхідних змін у контролі, політиці або процедурах.
- оцінка безпеки та авторизація. Визначення гарантії того, що вказані елементи керування виконуються правильно, працюють як задумано, і видають бажаний результат.
- планування форс-мажорів. Політики та процедури, призначені для підтримки або відновлення бізнес-операцій, включаючи комп'ютерні операції, можливо в альтернативному місці, у випадку надзвичайних ситуацій, збоїв системи або катастрофи.

– керування конфігураціями. Політики та процедури для контролю модифікацій апаратного забезпечення, прошивки, програмного забезпечення та документації для забезпечення захисту інформаційної системи від неналежних змін до, під час і після впровадження системи.
– ідентифікація та аутентифікація. Процес перевірки ідентичності користувача, процесу або пристрою за допомогою використання певних облікових даних (наприклад, паролів, жетонів, біометричних даних) як передумова для надання доступу до ресурсів в IT-системі.
– дії при інцидентах. Політики та процедури, які відносяться до тренування відповіді, тестування, керування, слідкування, звітності та підтримки роботи сервісів при інцидентах.
– підтримка. Політики та процедури для управління всіма аспектами підтримки інформаційної системи.
– захист носіїв даних. Політики та процедури для забезпечення безпечного зберігання даних. Контроль за доступом, маркуванням, зберіганням, транспортуванням, знищенням та переробкою носіїв даних.
– фізичний захист та захист довкілля. Політики та процедури, що стосуються фізичного доступу, доступу до передавання та відображення даних разом з контролем за середовищем роботи (кондиціонування, слідкування та вологістю повітря) та забезпечення продовольством у аварійних ситуаціях.
– планування. Розробка та підтримка плану забезпечення безпеки інформаційної системи шляхом виконання оцінок, визначення та впровадження засобів безпеки, призначення рівнів безпеки та реагування на інциденти.
– безпека персоналу. Політики та процедури категоризації, визначення придатності, транспортування, покарання та звільнення; також стосується зовнішніх служб безпеки.

– оцінка ризиків. Процес виявлення ризиків для операцій, активів або фізичних осіб шляхом визначення ймовірності виникнення, наслідків впливу та додаткового контролю безпеки, який би пом'якшив цей вплив.
– придбання систем та сервісів. Розподіл ресурсів для забезпечення безпеки інформаційних систем протягом всього життєвого циклу системи та розробки політики придбання на основі результатів оцінки ризиків, включаючи вимоги, критерії розробки, процедури тестування та супутню документацію.
– захист системи та комунікацій. Механізми захисту системи та засобів передавання даних.
– цілісність системи та інформації. Політики та процедури захисту інформаційних систем та їх даних від вад дизайну та заміни даних використовуючи перевірку функціональності, цілісності даних, вияву проникнення у систему, виконання шкідливого коду, попередження про небезпеку.
– програмне управління. Надає заходи управління безпекою на рівні всієї організації, а не тільки на інформаційно-системному рівні.

3.3 Захист локальної мережі АСУ ТП

Так, як сучасні інформаційні системи стають все складнішими та більшими у розмірах, для забезпечення їх безпеки, сервісу та підтримання працездатності часто використовують метод “розділяй та володій”, який полягає у розбитті однієї великої системи на кілька менших складових, які виконують одну, але конкретну функцію[14].

VLAN розділяють фізичні мережі на менші логічні мережі, щоб підвищити продуктивність, підвищити керованість і спростити дизайн мережі. VLAN досягається за допомогою конфігурації комутаторів Ethernet. Кожна VLAN складається з одного широкомовного домену, який ізолює трафік від інших

VLAN. Так само, як заміщення концентраторів комутаторами зменшує колізії, використання VLAN обмежує трансляцію трафіку, а також дозволяє логічним підмережам охоплювати декілька фізичних місць. Існують дві категорії VLAN:

- статичні, які часто називають порт-порт, де порти комутатора призначені для VLAN.
- динамічні, де кінцевий пристрій узгоджує характеристики VLAN з комутатором або визначає VLAN на основі IP або апаратних адрес.

Хоча більше однієї підмережі IP може співіснувати на одній VLAN, загальна рекомендація полягає у використанні відносин один-до-одного між підмережами та VLAN. Ця практика вимагає використання маршрутизатора або багатошарового комутатора для приєднання до декількох VLAN. Багато маршрутизаторів і брандмауерів підтримують позначені фрейми, так що один фізичний інтерфейс може використовуватися для маршрутизації між декількома логічними мережами.

VLAN, як правило, не розгортаються для вирішення вразливостей до хоста або мережі в способах розгортання брандмауерів або IDS. Проте, при правильному налаштуванні VLAN дозволяють комутаторам застосовувати політику безпеки та розділяти трафік на рівні Ethernet. Належним чином сегментовані мережі також можуть зменшити ризики штормів, які можуть виникнути в результаті сканування портів або активності черв'яків.

Комутатори були сприйнятливі до таких атак, як підробка MAC, переповнення таблиць і атаки проти протоколів основних дерев, залежно від пристрою та його конфігурації. Стрибання VLAN, здатність атаки вводити фрейми для несанкціонованих портів, було продемонстровано за допомогою спунінгу перемикання або подвійних інкапсульованих кадрів. Ці атаки не можуть проводитися віддалено і вимагають локального фізичного доступу до комутатора. Різні функції, такі як фільтрація MAC-адрес, аутентифікація на основі порту за допомогою IEEE 802.1x, і конкретні рекомендовані виробником методи можуть бути використані для пом'якшення цих атак, залежно від пристрою та реалізації.

3.4 Вимоги до персоналу АСУ ТП

Дуже важливо визначити та впровадити політику та процедури для забезпечення того, щоб всім користувачам інформаційної системи надавалися навчальні матеріали до надання дозволу на доступ до системи. Підготовку персоналу слід контролювати і документувати.

Для середовища АСУ ТП, це повинно включати в себе інформаційну безпеку, специфічну інформаційну безпеку системи та вивчення особливих для системи вимог. Окрім того, організація повинна ідентифікувати, документувати та навчати весь персонал, який має значні ролі та відповідальність у АСУ ТП. Поінформованість та навчання повинні охоплювати фізичний процес, що контролюється[15].

Усвідомлення безпеки є важливою частиною попередження інцидентів в АСУ ТП, особливо коли йдеться про загрози соціальної інженерії. Соціальна інженерія - це метод, який використовується для маніпулювання індивідуумами в наданні приватної інформації, наприклад, паролів. Ця інформація може бути використана для того, щоб скомпрометувати інші системи безпеки.

Реалізація програми безпеки АСУ ТП може змінити спосіб доступу персоналу до комп'ютерних програм, додатків і самого робочого столу комп'ютера. Організації повинні розробити ефективні навчальні програми та засоби комунікації, щоб допомогти співробітникам зрозуміти, чому потрібні нові методи доступу та контролю, ідеї, які вони можуть використовувати для зниження ризиків, та вплив на організацію, якщо методи контролю не включені. Програми навчання також демонструють прагнення керівництва до програми кібербезпеки та її цінність. Зворотній зв'язок від персоналу, що піддається такому типу навчання, може бути цінним джерелом інформації для уточнення статуту та обсягу програми безпеки.

3.5 Оцінка ризику та плани у випадку надзвичайних ситуацій

Незалежно від кроків, зроблених для захисту АСУ ТП, завжди можливо, що це може бути скомпрометовано навмисним або ненавмисним інцидентом. Наступні симптоми можуть виникати внаслідок нормальних мережевих проблем, але коли з'являються кілька симптомів, шаблон може вказувати на те, що система знаходиться під атакою і може бути варто дослідити далі. Якщо супротивник є кваліфікованим, то не зовсім очевидним є те, що атака триває.

Симптомами інциденту може будь-яка вказана нижче ситуація:

- незвичайно високий мережевий трафік
- закінчення місця на диску або його значне зменшення
- незвичайно велике використання центрального процесора
- створення нових облікових записів користувачів
- спроба або використання облікових записів рівня адміністратора
- блокування облікових записів
- використання облікового запису працівника, коли він не на роботі
- очищення журналу системи
- попередження антивірусного програмного забезпечення
- вимкнене антивірусне програмне забезпечення
- під’єднання до зовнішніх IP-адрес
- запити про інформацію про систему (спроби соціальної інженерії)
- неочікувані зміни у конфігурації
- неочікуване вимкнення системи

Щоб мінімізувати наслідки цих вторгнень, необхідно спланувати відповідь. Планування реагування на інциденти визначає процедури, яких слід дотримуватися, коли відбувається вторгнення. Посібник з керування інцидентами з комп'ютерною безпекою, надає вказівки щодо планування реагування на інциденти, які можуть містити такі елементи:

– класифікація інцидентів. Різні типи інцидентів АСУ ТП повинні бути ідентифіковані та класифіковані як потенційні наслідки, щоб можна було сформулювати відповідну реакцію для кожного потенційного інциденту
– відповіді на загрози. Є кілька відповідей, які можуть бути прийняті у випадку інциденту. Вони варіюються від бездіяльності до повного виключення системи (хоча повне вимкнення АСУ ТП є дуже малоймовірним). Відповідь буде залежати від типу інциденту та його впливу на АСУ ТП і контрольований фізичний процес. Необхідно підготувати письмовий план, що документує типи інцидентів та відповіді на кожен тип. Це дасть вказівки в часи, коли може виникнути плутанина або напруга через інцидент. Цей план повинен включати покрокові дії, які повинні виконувати різні організації. Якщо існують вимоги щодо звітності, їх слід зауважити, а також, де слід скласти звіт, та телефонні номери, щоб зменшити плутанину звітності
– дії з відновлення працездатності. Результати вторгнення можуть бути незначними, або вторгнення може спричинити багато проблем у АСУ ТП. Необхідно провести аналіз ризиків для визначення чутливості фізичної системи, яка контролюється, до режимів відмови в системі. У кожному випадку покрокові дії з відновлення повинні бути задокументовані таким чином, щоб система могла бути повернута до нормальних операцій якомога швидше і безпечніше. Дії відновлення для втручання, які впливають на роботу АСУ ТП, будуть тісно узгоджені з планом відновлення після аварії в системі, і повинні враховувати вже створене планування та координацію

Під час підготовки плану реагування на інциденти необхідно отримати інформацію від різних зацікавлених сторін, включаючи операції, інжиніринг, інформаційні технології, постачальники системної підтримки, управління, організовану працю, правову та безпечну діяльність. Ці зацікавлені сторони також повинні переглянути та затвердити план.

Необхідно запровадити офіційну програму управління змінами та застосувати процедури для того, щоб всі зміни в мережі системи відповідали тим самим вимогам безпеки, що й оригінальні компоненти, визначені в оцінці активів та пов'язані з ними плани оцінки ризиків і пом'якшення. Оцінка ризику повинна проводитися на всіх змінах мережі, які можуть вплинути на безпеку, включаючи зміни в конфігурації, додавання мережевих компонентів та встановлення програмного забезпечення. Також можуть знадобитися зміни в політиці та процедурах. Поточна конфігурація мережі АСУ ТП і конфігурації пристроїв повинні завжди бути відомими і задокументовані.

Плани на випадок надзвичайних ситуацій повинні охоплювати весь спектр невдач або проблем, які можуть бути спричинені кібер-інцидентами. Плани на випадок надзвичайних ситуацій повинні включати процедури відновлення систем від відомих дійсних резервних копій, відокремлення систем від усіх несуттєвих перешкод і з'єднань, які могли б дозволити вторгнення в кібербезпеку, і альтернативи для досягнення необхідних інтерфейсів і координації. Співробітники повинні бути навчені і знайомі з змістом планів на випадок надзвичайних ситуацій. Плани дій на випадок надзвичайних ситуацій повинні періодично переглядатися з працівниками, відповідальними за відновлення АСУ ТП, і перевірятися, щоб гарантувати, що вони продовжують виконувати свої цілі. Організації також мають плани безперервності бізнесу та плани відновлення після аварії, які тісно пов'язані з планами на випадок надзвичайних ситуацій.

Планування безперервності бізнесу вирішує загальну проблему збереження або відновлення виробництва у випадку переривання. Ці перерви можуть приймати форму стихійного лиха (наприклад, урагану, торнадо, землетрусу, повені), ненавмисної техногенної події (наприклад, випадкове пошкодження обладнання, пожежа або вибух, помилка оператора), умисне техногенне подія (наприклад, атака бомбою, вогнепальною зброєю або вандалізмом, зловмисником або вірусом) або збоєм обладнання. З точки зору потенційного відключення, це може включати типові часові проміжки днів, тижнів або місяців для відновлення після стихійного лиха або хвилини або години для відновлення після зараження

шкідливим програмним забезпеченням або механічної чи електричної несправності. Оскільки часто існує окрема дисципліна, що стосується надійності та електромеханічного обслуговування, деякі організації вибирають визначення безперервності бізнесу таким чином, що виключає ці джерела відмови. Оскільки безперервність бізнесу також стосується головним чином довгострокових наслідків відключень виробництва, деякі організації також вирішили розмістити обмеження на мінімальне переривання на ризики, які необхідно розглянути. Для цілей кібербезпеки АСУ ТП рекомендується не застосовувати жодного з цих обмежень. Довготривалі відключення (аварійне відновлення) та короткострокові відключення (оперативне відновлення) повинні бути розглянуті. Оскільки деякі з цих потенційних перерв пов'язані з техногенними подіями, важливо також співпрацювати з організацією фізичної безпеки, щоб зрозуміти відносні ризики цих подій та фізичні заходи безпеки, які існують для запобігання їх. Також важливо, щоб організація фізичної безпеки зрозуміла, в яких областях системи придбання та управління даними на виробничому майданчику міститься ризик більш високого рівня.

Після визначення цілей відновлення слід створити перелік потенційних перерв і розробити та описати процедуру відновлення. Для більшості перерв у менших масштабах ремонту та заміни діяльності на основі критичних запасів запасних частин буде достатньо для досягнення цілей відновлення. Коли це не відповідає дійсності, необхідно розробити резервні плани. У зв'язку з потенційними витратами та важливістю цих планів на випадок надзвичайних ситуацій, вони повинні бути переглянуті разом з керівниками, відповідальними за планування безперервності бізнесу, щоб переконатися, що вони є виправданими. Після того, як процедури відновлення будуть задокументовані, слід розробити графік для перевірки частини або всіх процедур відновлення. Особлива увага повинна приділятися перевірці резервних копій даних конфігурації системи та даних про продукт або продукцію. Приклади даних конфігурації системи включають в себе резервні копії конфігурації комп'ютера, резервні копії конфігурації програми, ліміти операційного контролю, контрольні смуги та задані

значення для операцій попереднього інциденту для всіх програмних пристроїв АСУ ТП. Вони не тільки повинні бути перевірені, коли вони виробляються, але й процедури, які слідують за їх зберігання, також повинні періодично переглядатися, щоб переконатися, що резервні копії зберігаються в умовах навколишнього середовища, які не зроблять їх непридатними і що вони зберігаються в безпечному місці, тому вони можуть бути швидко отримані уповноваженими особами, коли це необхідно.

3.6 Контроль доступу до АСУ ТП

Аутентифікація описує процес позитивної ідентифікації потенційних користувачів мережі, хостів, програм, служб і ресурсів, використовуючи комбінацію факторів ідентифікації або облікових даних. Результат цього процесу аутентифікації потім стає основою для дозволу або відмови від подальших дій (наприклад, коли банкомат запитує PIN-код). На основі визначення автентичності система може або не може дозволити потенційному користувачеві отримати доступ до своїх ресурсів. Авторизація - це процес визначення того, кому і що має бути дозволено мати доступ до певного ресурсу; контроль доступу - це механізм забезпечення авторизації.

Існує кілька можливих факторів для визначення автентичності особи, пристрою або системи, включаючи те, що ви знаєте, те, що у вас є або те, ким ви є. Наприклад, аутентифікація може бути заснована на чомусь, що ви знаєте (наприклад, PIN-код або пароль), чомусь, що ви маєте (наприклад, ключ, ключ, смарт-карта), тому, ким ви є як біологічна характеристика (наприклад, відбиток пальця, підпис сітківки), розташуванні (наприклад, доступ до системи глобального позиціонування). Загалом, чим більше факторів, які використовуються в процесі аутентифікації, тим надійнішим буде процес. При використанні двох або більше факторів процес відомий як багатофакторна аутентифікація.

Комп'ютерні системи в середовищі АСУ ТП зазвичай використовують традиційні паролі для автентифікації. Постачальники систем управління часто постачають системи з паролями за замовчуванням. Ці паролі встановлені на заводі і часто легко вгадуються або часто змінюються, що створює додаткові ризики для безпеки. Крім того, протоколи, які в даний час використовуються в середовищах АСУ ТП, зазвичай мають неадекватну або відсутність автентифікації мережевих послуг. На додаток до традиційних паролів, які використовуються в системах, доступні кілька форм аутентифікації. Деякі з них, включаючи аутентифікацію пароля, представлені в наступних розділах з обговоренням їх використання з АСУ ТП.

Якщо противник отримує доступ до носіїв резервної копії, пов'язаних з АСУ ТП, він може надати цінні дані для запуску атаки. Відновлення файлу аутентифікації з резервних копій може дозволити противнику запускати засоби для злому паролів і витягувати корисні паролі. Крім того, резервні копії зазвичай містять імена машин, IP-адреси, номери версій програмного забезпечення, імена користувачів та інші дані, корисні при плануванні атаки.

Використання будь-яких несанкціонованих компакт-дисків, DVD-дисків, дискети, USB-накопичувачів або подібних знімних носіїв на будь-якому вузлі, який є частиною або підключено до АСУ ТП, не допускається для запобігання впровадженню шкідливого програмного забезпечення або випадкової втрати або крадіжки даних. Якщо компоненти системи використовують немодифіковані промислові стандартні протоколи, механізоване програмне забезпечення для управління політикою може використовуватися для забезпечення політики захисту медіа.

Фізичний захист кібер-компонентів і даних, пов'язаних з АСУ ТП, має розглядатися як частина загальної безпеки заводу. Безпека в багатьох об'єктах системи тісно пов'язана з безпекою підприємства. Основна мета полягає в тому, щоб уникнути небезпечних ситуацій, не заважаючи їм виконувати свою роботу або виконувати надзвичайні процедури. Фізичні засоби безпеки - це будь-які фізичні заходи, активні або пасивні, які обмежують фізичний доступ до будь-яких

інформаційних ресурсів в середовищі АСУ ТП. Ці заходи застосовуються для запобігання багатьох видів небажаних ефектів, включаючи:

- фізичний доступ зловмисників до чутливих місць.
- фізична модифікація, маніпулювання, крадіжка або інше видалення або знищення існуючих систем, інфраструктури, комунікаційних інтерфейсів, персоналу або фізичних місць.
- несанкціоноване спостереження за чутливими інформаційними ресурсами через візуальне спостереження, записки, фотографії або інші засоби.
- запобігання несанкціонованому впровадженню нових систем, інфраструктури, комунікаційних інтерфейсів або іншого обладнання.
- запобігання несанкціонованому впровадженню пристроїв, навмисно створених для того, щоб викликати апаратні маніпуляції, підслуховування комунікацій або інші шкідливі наслідки.

Отримання фізичного доступу до контрольної кімнати або компонентів системи управління часто передбачає отримання логічного доступу до системи управління технологічними процесами. Крім того, наявність логічного доступу до систем, таких як основні сервери та комп'ютери контрольної кімнати, дозволяє противнику здійснювати контроль над фізичним процесом.

Якщо комп'ютери легкодоступні і вони мають знімні носії (наприклад, дискети, компакт-диски, зовнішні жорсткі диски) або USB-порти, приводи можуть бути оснащені замками або видалені з комп'ютерів, а USB-порти вимкнено. Залежно від потреб та ризиків безпеки, також може бути доцільним вимкнути або фізично захистити кнопки живлення для запобігання несанкціонованому використанню. Для максимальної безпеки сервери повинні бути розміщені в заблокованих областях і захищені механізми аутентифікації (такі як ключі). Крім того, мережеві пристрої в мережі АСУ ТП, включаючи комутатори, маршрутизатори, мережні роз'єми, сервери, робочі станції та контролери, повинні бути розташовані в захищеній зоні, до якої може бути доступ

тільки уповноважений персонал. Захищена зона також повинна бути сумісна з екологічними вимогами пристроїв.

Поглиблене рішення захисту фізичної безпеки має містити такі атрибути:

– захист фізичних локацій. Створення декількох фізичних бар'єрів, як активних, так і пасивних, навколо будівель, споруд, приміщень, обладнання або інших інформаційних ресурсів, встановлює ці фізичні периметри безпеки. Фізичні засоби безпеки, призначені для захисту фізичних місць, включають огорожі, протиударні канави, земляні кургани, стіни, посилені барикади, ворота або інші заходи. Більшість організацій включають цю багатошарову модель, запобігаючи першому доступу до заводу, використовуючи огорожі, охоронні лачуги, ворота і зачинені двері.

– контроль доступу. Системи контролю доступу повинні забезпечити доступ тільки до уповноважених осіб до контрольованих просторів. Система контролю доступу повинна бути гнучкою. Потреба в доступі може базуватися на часі (денна або нічна зміна), рівні підготовки, статусу зайнятості, призначення на роботу, статусі рослин і безлічі інших факторів. Система повинна бути в змозі перевірити, що особа, якій надано доступ, є тією, ким її вважають (зазвичай використовують те, що особа має, наприклад картку доступу або ключ, те, що знає, наприклад, ідентифікаційний номер (PIN-код) або щось інше, використовуючи біометричний пристрій). Контроль доступу повинен бути високонадійним, але не заважати рутинним або аварійним обов'язкам персоналу заводу. Інтеграція системи контролю доступу в технологічну систему дозволяє розглядати не тільки безпечний доступ, але й фізичне та кадрове відстеження активів, різко прискорюючи час реагування в надзвичайних ситуаціях, допомагаючи спрямувати людей до безпечних місць і підвищуючи загальну продуктивність. В межах району доступ до мереж і комп'ютерних шаф повинен обмежуватися лише тими, у кого є

потреба, наприклад, мережеві техніки та інженери, або персонал з обслуговування комп'ютерів. Шафи обладнання повинні бути заблоковані, а електропроводка повинна бути акуратною. Розглядають також можливість збереження всіх комп'ютерів у захищених стійках та використання технології розширення периферійних пристроїв для підключення інтерфейсів людини та машини до комп'ютерів, що використовуються у стійкому стані.

– система слідкування за доступом. Системи контролю доступу включають камери і відеокамери, датчики та різні типи систем ідентифікації. Прикладами таких систем є камери, які контролюють стоянки чи магазини. Ці пристрої спеціально не запобігають доступу до певного місця розташування; скоріше, вони зберігають і фіксують фізичну присутність або відсутність фізичної присутності осіб, транспортних засобів, тварин або інших фізичних осіб. Належне освітлення повинно бути забезпечене на основі типу пристрою моніторингу доступу.
– системи обмеження доступу. Системи обмеження доступу можуть використовувати комбінацію пристроїв для фізичного контролю або запобігання доступу до захищених ресурсів. Системи обмеження доступу включають як активні, так і пасивні пристрої безпеки, такі як огорожі, двері, сейфи, ворота та охоронні пристрої. Вони часто поєднуються з системами ідентифікації та моніторингу для забезпечення рольового доступу для конкретних осіб або груп осіб.
– відслідковування людей та активів. Розміщення людей та транспортних засобів у великих об'єктах є дуже важливим з міркувань безпеки. Технології розміщення активів можуть бути використані для відстеження переміщень людей і транспортних засобів на заводі, для забезпечення їх перебування в дозволених зонах, для визначення персоналу, який потребує допомоги, і для підтримки реагування на надзвичайні ситуації.

– фактори навколишнього середовища. При вирішенні проблем безпеки системи та даних важливо враховувати фактори навколишнього середовища. Наприклад, якщо підприємство знаходиться у запиленому середовищі, системи повинні бути розміщені у фільтрованому середовищі. Це особливо важливо, якщо пил, ймовірно, є провідним або магнітним, як у випадку з вузлами, які обробляють вугілля або залізо. Якщо присутня вібрація, системи повинні бути встановлені на гумових втулках, щоб запобігти виникненню проблем з дисками та з'єднанням. Крім того, середовища, що містять системи та носії (наприклад, резервні стрічки, дискети), повинні мати стабільну температуру та вологість. Сигнал для системи керування технологічними процесами повинен генеруватися, коли перевищуються такі характеристики навколишнього середовища, як температура та вологість.
– системи контролю за навколишнім середовищем. Системи опалення, вентиляції та кондиціонування повітря для контрольних приміщень повинні підтримувати персонал під час нормальної експлуатації та аварійних ситуацій, які можуть включати викид токсичних речовин, у оптимальному середовищі. Пожежні системи повинні бути ретельно розроблені, щоб уникнути більшої шкоди, ніж користі (наприклад, щоб уникнути змішування води з несумісними продуктами).
– електрозабезпечення. Надійне живлення для АСУ ТП має важливе значення, тому необхідно забезпечити безперебійне живлення. Якщо на місці є аварійний генератор, тривалість роботи батареї аварійного живлення може становити лише кілька секунд; однак, якщо підприємство покладається на зовнішнє живлення, час роботи такої батареї має складати не менше кількох годин.

Висновки до розділу 3

Прихильність до програми безпеки починається зверху. Вище керівництво повинно продемонструвати чітку прихильність до інформаційної безпеки. Інформаційна безпека є діловою відповідальністю, яку поділяють всі члени підприємства і особливо провідні члени бізнесу, процесів і керівних команд. Програми інформаційної безпеки з достатнім фінансуванням і видимою підтримкою на вищому рівні з боку лідерів організацій, швидше за все, досягають відповідності, функціонують більш гладко, і мають більший успіх, ніж програми, які не мають такої підтримки.

Коли розробляється та встановлюється нова система, обов'язково потрібно витрачати час на забезпечення безпеки протягом усього життєвого циклу, від архітектури до закупівлі, установки, обслуговування та виведення з експлуатації. Існують серйозні ризики при розгортанні систем до виробництва, виходячи з припущення, що вони будуть забезпечені пізніше. Якщо часу та ресурсів недостатньо для належного забезпечення системи належним чином перед розгортанням, малоймовірно, що пізніше буде достатньо часу та ресурсів для вирішення питань безпеки.

ВИСНОВКИ

У цьому дипломному проекті було глибоко досліджено автоматизовані системи управління технологічним процесом у контексті їх взаємодії з загрозами. Було визначено основі загрози, властиві таким системах, обґрунтовано причини їх появи, досліджено їх вплив на систему та можливі шкідливі наслідки, розроблена методика побудови систем захисту критичних інформаційних ресурсів.

Також було побудована математична модель впливу загроз на інформаційну систему, яка може знаходитись у 4-х станах:

1. Загроза не поступала і, відповідно, не була реалізована
2. Загроза поступала, але не була реалізована
3. Загроза поступила та була реалізована
4. Загроза поступила, але була відбита системою захисту

Наведено два приклади обрахування ймовірності знаходження системи у кожному з станів.

У останньому розділі увага зверталась на практичне використання автоматизованих систем управління технологічним процесом з нахилом до безпеки. Були описані виклики, недоліки та переваги, які з’являються при виділенні особливої уваги саме безпеці таких систем.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. Олифер, Н. Олифер. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2015. – 944 с.

2. Астахов А.А., Особенности обеспечения информационной безопасности промышленных систем/ А. Астахов // CISA-2006. - No3. - С. 76-79.

3. Куприянов А.И., Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений/ А.И. Куприянов, А.В. Сахаров, В.А. Шевцов// - М.: Издательский центр «Академия», 2006. - 256 с.

4. Галатенко, В.А. Основы информационной безопасности: курс лекций; учеб. Пособие. Издание третье / В.А. Галатенко; под ред. Академика РАН В.Б. Бетелина. - М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. - 208 с.

5. Галкин А.П., Защита каналов связи предприятий и учреждений от несанкционированного доступа к информации: учеб. пособие / А.П. Галкин. - Владимир: Изд-во ВлГУ, 2003. - 128 с.

6. Шувалов И.А., Росенко А.П. Имитационная мо- дель реализации внутренних и внешних угроз безопасности информационной системы на сегменте «коммутатор – сер- вер» // Вестник Дагестанского государственного универси- тета. – 2013. – Вып. 1. – С. 112–123.

7. Теоретические основы анализа иоценки влияния внутренних угроз на безопасность конфиденциальной ин- формации: монография / А.П. Росенко. – М.: Гелиос АРВ, 2008. – 154 с.

8. Шувалов И.А., Семенчин Е.А. Имитационная мо- дель реализации внутренних и внешних угроз безопасности
информационной системы на сегменте «Маршрутизатор – маршрутизатор» // Фундаментальные исследования. – 2012. – No 9. – С. 425–431.

9. Leite, M.D., Marczal, D. Pimentel, A.R. 2013, ”Multiple external representations in remediation of math errors”, ICEIS 2013 - Proceedings of the 15th International Conference on Enterprise Information Systems, pp. 519.

10. Yang, D. 2013, Empirical analysis of the demand for interpretation system of world cultural heritage based on optimized selection model and mathematical physics equations.

11. Правила для безпеки інформаційних систем та мереж: До культури безпеки 2016. [Електронний ресурс] – Режим доступу до ресурсу: http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD guidelines.pdf.

12. Schjolberg S., Ghernaouti-Hlie S. Глобальний договір про кібербезпеку та кіберзлочинство, Друге видання. [Електронний ресурс] – Режим доступу до ресурсу: http://www.cybercrimelaw.net/documents/.

13. Висновок з відповідей на опитуванні про впровадження правил безпеки інформаційних систем та мереж: до культури безпеки 2012. [Електронний ресурс] – Режим доступу: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2003)8 /FINAL&docLanguage=En.

14. Політика кібербезпеки на роздоріжжі. Аналіз нового покоління стратегій кібербезпеки. [Електронний ресурс] – Режим доступу до ресурсу: http://www.oecd.org/officialdocuments/.

15. Керування ризиками інформаційної безпеки для соціального та економічного процвітання. [Електронний ресурс] – Режим доступу до ресурсу: http://dx.doi.org/10.1787/9789264245471-en.

ДОДАТОК А

Таблиця А.1 – Порівняння найпопулярніших SCADA-систем

	SIMATIC WINCC	INTOUCH	OpenSCADA
Ведення архіву подій	+	+	+
Захист налаштувань паролем	+	+	+
Наявність різних прав доступу користувачів	+	+	+
Налаштування дозволеного часу входу для користувачів	+	+	-
Гаряче резервування	+	+	+
Віддалене перезавантаження контролерів	+	+	-
Синхронізація системного часу	+	+	+
Самотестування, знаходження помилок	+	+	+

Продовження таблиці А.1

	SIMATIC WINCC	INTOUCH	OpenSCADA
Повідомлення про тривогу на екрані	+	+	+
Звукове повідомлення про тривогу	+	+	+
Функція сторожового таймеру	+	+	+
Автоматичний старт/перезапуск системи у випадку помилки	+	+	+
Інформація про помилки комутації	+	+	+
Автоматичний контроль вільної пам’яті на диску	+	+	-
Відновлення заводських налаштувань та параметрів	+	+	+

Продовження таблиці А.1

	SIMATIC WINCC	INTOUCH	OpenSCADA
Контроль достовірності параметрів вимірювання	+	+	+
Контроль допустимості інформації, яку вводить оператор	+	+	+
Блокування визначених команд в аварійній ситуації	+	+	+
Контекстна допомога в управлінні	+	+	-
Інтуїтивний графічний HMI-інтерфейс	+	+	+